H3C

数字化及AI解决方案领导者

智能体时代网络软件架构技术白皮书

Agentic Network Software Architecture Technical White Paper

www.h3c.com

目录

第一章 智能体时代网络软件的几大变革 1

接口交互范式演进: REST API到MCP

协作范式演进: 从传统消息到A2A

业务流程范式演进: Workflow到Skills

人机交互演进: GUI到Canvas

第二章 智能体时代网络软件架构设计 5

工作空间层

技能工具层

数据感知层

基础设施层

第三章 智能体时代网络软件最佳实践 9

知识问答: 提问获取准确答案

态势查询: 设备巡检与可视化报告

智能排障: 终端信号差故障定位

智能调优: 无线射频调优

目录

第四章 新华三网络智能体架构 22

整体架构

网络智能体业务规划双引擎

支持客户自有智能体

第五章 H3C网络智能体部署 26

公有云部署

本地部署

第六章 网络智能体未来蓝图 28

多智能体协同

原生智能的网络设备

人机审核与自我进化

序

网络是数字化时代的神经系统。从企业办公到云计算，从智能制造到智慧城市，每一比特数据的流转都依赖网络的承载与调度。而网络管理软件，正是守护这一庞大神经系统健康的核心器官。数十年来，网络软件经历了从命令行到图形界面、从单机到云端、从人工到自动化的持续演进，每一次技术变革都深刻重塑了网络运维的范式与效率。

今天，我们正站在又一个变革的拐点上。以大语言模型为代表的人工智能技术，正在催生一种全新的软件形态——智能体（AI Agent）。智能体不同于传统的程序，它具备理解意图、自主规划、调用工具、反思修正的能力，能够在开放环境中完成复杂的任务目标。当智能体技术与网络管理相遇，一场深刻的范式转换正在发生：API接口从REST走向MCP，服务通信从消息队列走向A2A，业务流程从刚性工作流走向Agentic Skills，人机交互从固定GUI走向动态Canvas。这四大变革不是孤立的技术升级，而是相互关联、彼此支撑的系统重构，共同指向一个愿景——让网络运维更智能、更高效、更人性化。

本白皮书的撰写基于业界前沿的技术研究和实践探索。我们深入分析了MCP、A2A等开放标准的技术细节，借鉴了ReAct、RAG、Agentic Workflow等先进的智能体架构模式，并结合网络管理领域的特殊需求进行了针对性的设计与适配。

智能体时代网络软件的几大变革

随着大语言模型（LLM）技术的快速演进，人工智能正在从简单的对话助手进化为能够自主规划、执行和反思的智能体（Agent）。这一变革性趋势正在深刻重塑网络管理软件的技术栈和架构范式。传统网络软件基于确定性规则、静态编排和固定界面的设计哲学，已难以适应云原生、边缘计算和意图驱动网络等新场景的需求。智能体时代的到来，为网络软件带来了四大根本性变革。

接口交互范式演进：REST API到MCP

传统网管系统通过RESTful API实现与网络设备、北向应用和外部系统的交互。REST API虽然成熟稳定，但其设计哲学围绕"资源"的概念展开，强调无状态、可缓存和统一接口。当AI智能体需要与网络基础设施交互时，REST API面临几个根本性挑战：API发现困难（智能体难以理解海量API的语义）、上下文传递受限、工具调用缺乏标准化。

Model Context Protocol（MCP）由Anthropic于2024年推出，现已成为Linux基金会Agentic AI Foundation（AAIF）旗下的开放标准。MCP通过客户端–服务器架构，为AI智能体提供了标准化的工具发现、认证和调用机制。截至2026年初，MCP月SDK下载量已突破9700万次，社区活跃服务器超过10000个（数据来源：Anthropic 捐赠公告（2025-12-09）），已成为事实上的智能体-工具交互标准。MCP将M乘以N的集成复杂度降低为M加N，每个模型和工具只需一个MCP适配器即可实现互操作。

在网管场景中，MCP Server可以封装网络设备、监控系统的配置、查询API和自动化脚本的执行入口，将底层的RESTful API转换为智能体友好的高层工具抽象。智能体通过MCP Client动态发现可用工具，根据任务需求自主选择合适的工具进行调用。这一范式转变使得网管系统的开放接口从“面向开发者”演进为“面向智能体”，大大降低了AI与网络基础设施的集成门槛。

协作范式演进：从传统消息到A2A

传统分布式系统中的服务间通信依赖消息队列、RPC或事件总线等机制。这些协议虽然成熟可靠，但主要服务于确定性、编排式的工作流程。在智能体时代，多个自主智能体需要协同工作时，传统消息机制面临新的挑战：智能体间缺乏标准化的能力发现机制、任务委托语义不明确、多轮对话和异步协作缺乏规范。

因此，A2A协议（Agent-to-Agent Protocol，智能体到智能体协议）应运而生。A2A并不替代消息队列、RPC 等底层通信组件，它是构建在现有通信底座之上、面向智能体业务语义的上层标准。A2A协议由Google于2025年4月推出，并捐赠给Linux基金会。A2A定义了智能体间协作的开放标准，核心概念包括：Agent Card（JSON格式的能力描述文档，发布在well-known URL上）、Task（有状态的工作单元，包含完整的生命周期管理）、Message和Part（结构化的通信载体）以及Artifact（智能体产出的结构化输出）。截至2026年8月，官网合作伙伴页已列 170+家组织（数据来源：Linux基金会官方新闻稿（2026-04-09，A2A 一周年）），包括Google、Microsoft、AWS、Salesforce、SAP等。

在网管场景中，A2A使得不同厂商、不同框架的网络管理智能体能够无缝协作。例如，监控智能体发现异常后，可以通过A2A协议委托诊断智能体进行根因分析；诊断完成后，再由配置智能体执行修复操作。每个智能体保持自主性，无需暴露内部逻辑和状态，仅通过标准化的Agent Card声明自身能力。这种“去中心化”的协作模式相比传统的集中式编排，具有更高的灵活性和可扩展性。

业务流程范式演进：Workflow到Skills

传统网管系统的业务流程采用预定义的工作流（Workflow）模式，由工程师通过图形化工具或脚本编排固定的步骤序列。这种模式适用于确定性强、规则明确的场景，但在面对复杂多变的网络环境时，刚性工作流往往力不从心：分支逻辑难以穷尽、异常处理需要大量预判、新场景适配成本高。

Agentic Skills（智能体技能）代表了业务流程编排的范式转变。Skill是可复用的能力单元，由自然语言描述、工具集合、执行策略和验证规则组成。与刚性工作流不同，Skills赋予智能体动态规划和自主决策的能力。智能体接收用户意图后，结合可用Skills进行任务分解，选择最合适的工具组合，并在执行过程中根据反馈进行自适应调整。

在网管场景中，Skills可以包括：设备巡检技能（自动登录设备、执行检查命令、分析输出结果）、配置合规技能（比对当前配置与基线、识别偏差、生成修复建议）、故障诊断技能（收集告警信息、关联分析、定位根因）。这些Skills可以通过自然语言描述进行组合和复用，工程师只需关注“做什么”而非“怎么做”，具体执行策略由智能体根据实时环境动态决定。

ReAct（Reasoning + Acting，推理与行动）模式是实现Agentic Skills的核心架构。ReAct通过Thought–Action–Observation（思考–行动–观察）的迭代循环，使智能体能够在思考中行动、在行动中反思。当执行网络故障排查任务时，智能体首先分析当前状况（Thought），然后选择合适的诊断工具（Action），观察执行结果（Observation），再根据反馈调整下一步策略。这种闭环推理机制使智能体能够处理开放性、探索性的运维任务。

人机交互演进：GUI到Canvas

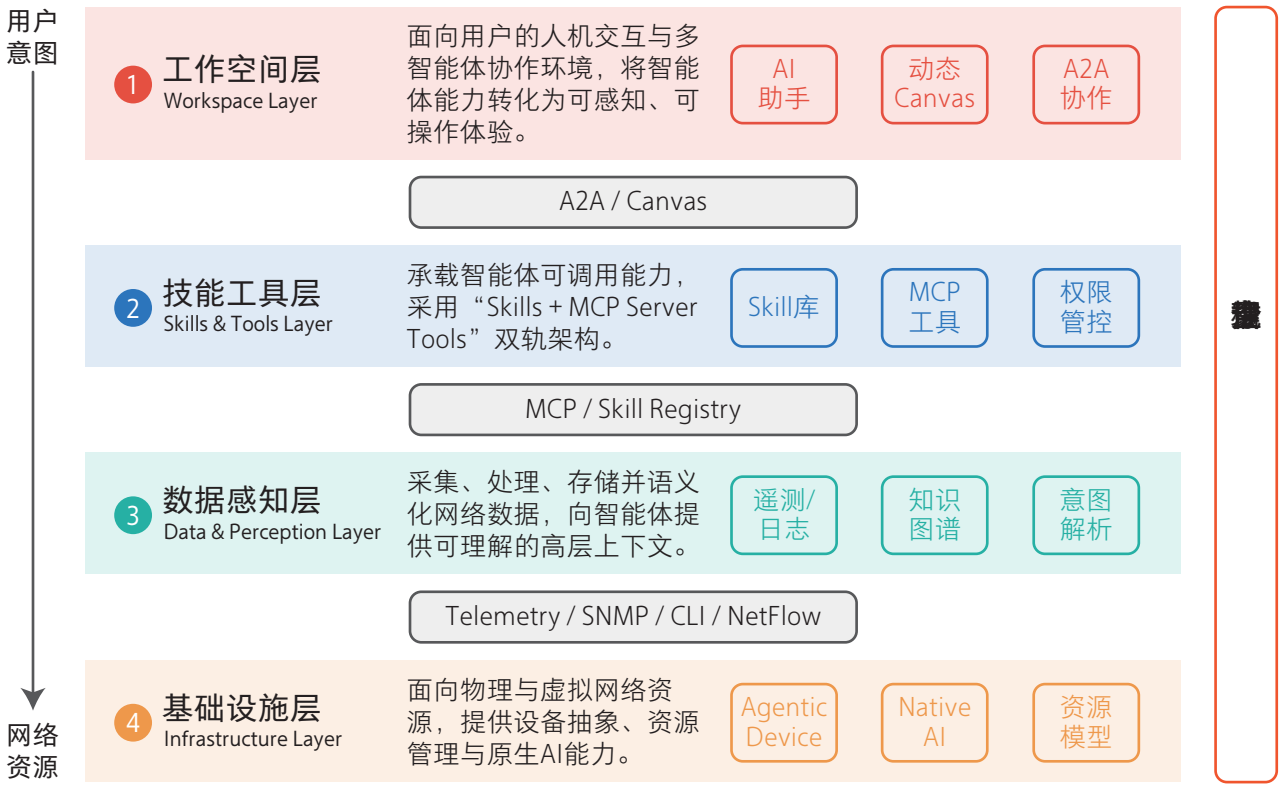
传统网络软件依赖图形用户界面（GUI）进行人机交互，通过菜单、按钮、表单和仪表板等固定元素提供操作入口。GUI模式虽然直观易用，但在AI时代面临根本性限制：交互模式僵化（预设的UI元素难以覆盖所有场景）、信息密度受限、上下文割裂（用户需要在多个界面间切换）。

Canvas（画布）模式代表了人机交互的范式革新。Canvas是一个开放的、可动态生成的协作空间，智能体根据用户意图和任务上下文，实时生成操作界面元素。OpenAI的ChatGPT Canvas、Amazon 的 Canvas 类产品等展示了这一模式的巨大潜力。在Canvas中，用户通过自然语言下达指令，智能体理解意图后动态生成相应的交互界面：数据分析任务自动生成图表、配置任务生成表单、排障任务生成拓扑图。

在网管场景中，Canvas模式带来了革命性的交互体验。运维人员可以通过自然语言询问"展示北京XX园区的流量趋势"，智能体理解语义后调用MCP工具获取数据，在Canvas上动态生成可视化图表；当发现异常时，运维人员可以继续追问"分析异常原因"，智能体在现有Canvas上追加诊断信息和修复建议。整个交互过程流畅自然，无需切换界面或学习复杂的操作路径。Canvas使网络软件从“人适应系统”转变为“系统适应人”。

智能体时代网络软件架构设计

基于前述四大变革，智能体时代的网络软件需要采用全新的分层架构。该架构自上而下分为工作空间层、技能工具层、数据感知层和基础设施层，各层之间通过标准化协议松耦合连接，形成完整的智能体网络技术栈。



工作空间层

工作空间层是智能体系统的最顶层，直接面向用户，提供人机交互和多智能体协作的环境。该层的核心使命是将智能体的能力转化为用户可感知、可交互的直观体验。

使用AI助手或画布等形式与用户进行交互；根据AI输出信息渲染数据图表（如趋势图、拓扑图），并按需生成操作框、按钮等。

技能工具层

技能工具层是智能体能力的承载层，负责封装和管理智能体可调用的技能和工具。该层采用Skills加MCP Server Tools的双轨架构：Skills面向业务语义，定义智能体在特定领域的专业能力；MCP Server Tools面向技术实现，提供标准化的工具调用接口。

Skills体系采用三层结构：基础技能层提供SSH连接、SNMP查询、日志解析、NetFlow采集等通用网络操作能力，是所有上层技能的基石；领域技能层提供路由诊断、流量分析、配置审计、安全合规检查等专业能力，面向特定的网络技术领域；场景技能层提供割接保障、应急演练、变更审批、巡检报告等完整的业务场景能力，通常由多个领域技能组合而成。每个Skill包含自然语言描述（供智能体理解其用途和适用场景）、输入输出规范（定义参数和返回值的格式）、依赖工具列表和验证规则（确保执行结果的正确性）。Skill之间支持组合和继承，形成灵活的能力体系。

MCP Server Tools层将底层基础设施的能力封装为智能体可调用的标准化工具，例如，已有的智能运维功能（如终端智诊、网络智诊等）可以封装为MCP Server中的一个接口，智能体即可理解并在需要的时候使用。每个MCP Server专注于一类网络资源或操作领域：设备管理Server提供配置下发、状态查询、命令执行、固件升级等工具，支持SSH、Netconf等多种管理协议；监控Server提供指标查询、告警管理、阈值设置、仪表盘操作等工具，对接Prometheus、Zabbix、Grafana等监控系统；自动化Server提供脚本执行、工作流触发、结果收集、定时任务管理等工具，支持Ansible、

Python脚本等自动化手段。所有MCP Server遵循统一的协议规范，任何兼容的MCP Client都可以自动发现、动态调用其工具。

Skill Registry（技能注册中心）是技能工具层的治理枢纽，负责Skills的发现、版本管理和权限控制。新开发的Skills注册到注册中心后，智能体可以自动发现和使用。注册中心支持语义搜索，智能体可以通过自然语言描述找到最合适的Skill。版本管理确保升级过程中向后兼容，支持灰度发布和快速回滚。权限控制机制基于RBAC模型，确保只有授权的智能体才能调用敏感Skills。

数据感知层

数据感知层是智能体与基础设施之间的数据桥梁，负责网络数据的采集、处理、存储和语义化。该层的核心目标是将底层异构的网络数据转换为智能体可理解和使用的高层语义信息。

基础设施交互协议是数据感知层的基础。该层采用多模态数据采集架构，支持Streaming Telemetry（遥测数据推送）、 Syslog（日志收集）、SNMP（传统设备监控）、CLI（命令行交互）、NetFlow或sFlow（流量分析）、BGP BMP（路由监控）等多种数据采集协议。采集引擎通过MCP Server Tools接收智能体的数据请求，自动选择最合适的采集方式和参数。例如，当智能体需要获取设备接口流量时，引擎优先选择Streaming Telemetry获取实时数据，如不支持则回退到SNMP轮询。采集到的原始数据经过解析、归一化和富化处理后，存入统一的数据平台。

知识图谱是数据感知层的核心智能组件。网络知识图谱将设备、接口、链路、业务、租户、IP地址段等网络实体及其关系建模为图结构，为智能体提供结构化的领域知识。图谱中的节点代表网络实体，边代表实体间的关系（如设备包含接口、接口连接链路、链路承载业务等）。当智能体执行故障诊断任务时，知识图谱支持快速的相关性分析（哪些业务受到故障影响）和影响范围评估（故障会波及哪些租户和设备）。知识图谱还与LLM结合，通过检索增强生成（RAG）技术为大模型提供准确的领域上下文，显著降低幻觉风险。

语义理解和意图解析模块负责将自然语言查询转换为结构化的数据请求。当用户询问“展示过去一小时核心交换机CPU利用率最高的三台设备”时，语义理解模块解析出时间范围（过去一小时）、对象（核心交换机）、指标（CPU利用率）、排序方式（从高到低）和限制条件（三台），然后生成对应的数据查询语句。该模块采用LLM加规则引擎的混合架构，LLM负责理解自然语言的灵活表达，规则引擎负责确保生成的查询符合数据模型的约束。

基础设施层

基础设施层是智能体网管系统的最底层，直接面向物理和虚拟网络资源。在智能体时代，基础设施层不仅需要提供传统的网络管理能力，还需要支持Agentic Device和Native AI两大新兴能力。

Native AI（原生AI能力）指在网管系统核心组件中内嵌AI能力，而非作为外挂模块。这包括：AI驱动的配置验证引擎，在配置下发前通过AI模拟验证，预测潜在风险（如无线弱覆盖、无线干扰高、环路、黑洞、ACL冲突）；AI增强的告警关联分析，自动识别告警间的因果关系，过滤噪音，将数十个相关告警聚合为一个根因事件；AI辅助的容量规划，基于历史数据和业务趋势进行智能预测，提前预警资源瓶颈。Native AI使网管系统具备“内建智能”，而非依赖外部AI的“外挂智能”，从根本上提升了系统的自主决策能力。

Agentic Device（智能体设备）是新一代网络设备的演进方向。这类设备内置AI推理能力，支持通过MCP Server直接暴露管理接口，无需外部控制器即可与智能体交互。设备内置的AI引擎可以在本地进行实时分析，仅在需要时与云端智能体协作。这种边缘到云协同架构既保证了实时性，又充分利用了云端强大的推理能力。

基础设施层还包含设备抽象和资源管理组件。设备抽象层通过统一的资源模型屏蔽不同厂商、不同型号设备的差异，为上层智能体提供一致的资源视图和操作接口。无论是H3C设备还是第三方设备，智能体都通过相同的抽象接口进行操作。资源管理组件负责设备生命周期管理（纳管、变更、退网）、软件版本管理（基线定义、升级调度、版本回退）、配置基线管理（模板定义、合规检查、偏差修复）和策略管理，为上层智能体提供稳定可靠的资源管理底座。

智能体时代网络软件最佳实践

以下四个典型场景展示了智能体网络架构在实际运维中的落地实践，覆盖了知识问答、态势查询、智能排障和网络优化四类核心运维活动。

知识问答：提问获取准确答案



场景描述

某用户对Cloudnet配置云AP的操作不熟悉；传统方式是到官网查找相关资料，需要十分钟。

运维人员通过自然语言向智能体提问，直接获取准确信息。



智能体
解决方案

执行过程分为三个阶段。第一阶段是意图解析：判断意图为知识问答；第二阶段是补齐信息并查询知识库：将用户在向Cloudnet灵犀AI助手发出的提问，补齐为Cloudnet云AP配置模板，然后通过多路并行召回获取知识库内容；第三阶段是检索结果处理与信息输出：判断内容信息充分性，是则输出结果；否则进行二次检索。

用户输入“如何配置云AP模板？”，20秒内即可获取准确结果。

如何配置云AP模板？



knowledge_search 完成

根据云简知识库的资料，以下为您详细介绍**云AP模板**的配置方法：

云AP模板配置（云简平台）

云AP模板可以批量配置和下发Wi-Fi设置到多个场所的云AP上，适用于设备数量较多的场景。

操作路径

网络管理 > 配置 > 批量模板 > 云AP模板

配置步骤

1. 创建模板

1. 点击 **<增加>** 按钮进入云AP模板配置页面
2. 配置 **模板名称** 和 **描述信息**

2. 配置Wi-Fi

在 **"Wi-Fi配置"** 页签下，开启 **状态** 开关，配置以下内容：

- **SSID名称** — 终端看到的无线网络名称
- **加密服务** — 可选 PSK（需配置密码）/ 802.1X（需认证服务器）/ 关闭（开放）
- **高级配置**：
  - 服务状态（开启/关闭）
  - 隐藏SSID
  - 二层隔离
  - 转发模式
  - 带宽保障等

配置完成后点击 **<保存>**

3. 命令行配置（可选）

在 **"命令行配置"** 页签下，开启状态开关，可向云AP下发自定义命令行：

- 先选择云AP型号（或全部型号）
- 参考举例栏输入命令行（需先进入系统视图）
- 每个模板最多支持10个配置片段
- 点击 **<确定>** 下发

4. 应用模板

1. 返回云AP模板列表页
2. 找到创建的模板，点击操作栏的 **应用** 图标
3. 选择目标分支和场所
4. 点击 **<应用>** 按钮批量下发到场所下的在线云AP

5. 查看应用结果

- 点击操作栏的 **历史** 图标查看应用记录
- 如果部分设备应用失败，可点击 **<重新应用>** 重试

请问您是想在哪个场所配置云AP模板？需要我帮您查看当前场所的云AP设备情况吗？

输入 111286 输出 540 共 111826 tokens 19.6s

态势查询：设备巡检与可视化报告

某企业网络运维团队需要对全国数十个园区的网络设备进行例行巡检，并生成可视化巡检报告供管理层审阅。传统方式下，工程师需要逐一登录设备、执行检查命令、手动整理结果、制作报告，整个过程耗时数小时。



场景描述

运维人员通过自然语言下达指令“对所有场所进行全面巡检，生成包含设备状态、性能趋势、风险提示的可视化报告”。智能体理解意图后，自动进入巡检工作流。



智能体
解决方案

执行过程分为四个阶段。第一阶段是任务分解与并行执行：智能体将巡检任务分解为三个并行的子任务（每个园区场所一个），每个子任务进一步分解为设备状态采集、性能指标查询、告警/风险检查三个并行的操作。多个园区场所的巡检任务同时执行，大幅缩短总体耗时。

第二阶段是数据采集与处理：各子任务通过MCP 调用获取采集网络容量、设备运行态势（例如，硬件状态、接口流量、CPU内存利用率、温度、无线信号质量）、用户体验态势等关键指标。采集到的原始数据经过归一化处理和异常检测，识别出偏离基线的指标项。

第三阶段是可视化报告生成：根据采集到的数据，在工作空间中动态生成可视化报告。报告包括：执行摘要（整体健康度评分和关键发现）、设备状态矩阵（所有设备的运行状态一览）、风险优先级列表（需要关注的问题按严重程度排序）等。

用户只需下发对话：“巡检所有场所”，即可获取巡检结果。耗时减少到几十秒。

📋 全场所巡检报告

巡检时间： 2026-08-25 17:08

🏢 1. 研发黄区（shopId: ）

AC设备： 2台（AC-HUANGQU、AC-YANFA）— 全部在线 🟢 **AP：** 2台 — 全部在线，评分100

AP	型号	终端数	信号问题
0086-2023-2010	WA7220	**6台**	⚠ 5台终端信号 **-83dBm**（弱）
huangqu_q	WA7220	**3台**	✅ 信号良好 -35~-39dBm
终端总计：9台 — 全部5GHz，健康评分100			

🏢 2. 行政区一楼（shopId: ）

AC设备： 2台（AC-ADMIN-1F、AC-XINGZHENG）— 全部在线 🟢 **AP：** 15台 — 全部在线，评分100 **终端总计：29台** — 全部5GHz，健康评分100

- **AP-CORE** 承载约15台终端，信号范围-24~-47dBm
- **AP-HF-WEAK** 下3台终端信号-83dBm ⚠
- 认证方式：多数未认证，部分MAC地址认证

🏢 3. 红枫大楼（shopId: ）

AC设备： 2台（AC-HONGFENG、AC-REDFENG）— 全部在线 🟢 **AP：** 6台 — 全部在线，评分100 **终端总计：48台** — 全部5GHz，健康评分100

- ⚠ **AP-HF-WEAK** 下3台终端信号均为 **-83dBm**（弱覆盖）
- ⚠ **AP-HF-OVERLOAD** 承载 **40台终端**，负载较高
- 其余AP信号良好

🏢 4. TestAI场所（shopId: ）

AC设备： 1台（AC-TESTAI）— 在线 🟢 **AP：** 1台（TestAI-AP-1）— 在线，评分100 **终端：3台** — 信号-26~-34dBm，良好 ✅

🏢 5. new（shopId: ）

AC设备： 1台（CAP-2，WX5540H）— **离线** 🔴 **AP：** 无 **终端：** 无 ⚠ 该场所唯一设备离线，需关注

---

6. Changhe Road（shopId: ）

AC设备： 1台（AC-CHANGHE）— 在线 🟢 **AP：** 8台 — 全部在线，评分100 **终端总计：27台** — 全部5GHz，健康评分100

- ⚠️ **AP-CHANGHE-RRM** 下大量终端信号 **-83dBm**（弱覆盖）
- **bangong_X_B** 下2台终端信号 **-83dBm**
- **changhe_wkcov_01** 下4台终端信号 **-83dBm**
- **AP-CHANGHE-1TERM** 下1台终端信号 **-83dBm**
- 仅 **changhe7lou-AP-guaijiao**、**changhe_good_01** 信号良好 ✅

📊 全场所汇总

场所	AC	AP总数	在线AP	终端数	异常告警
研发黄区	2台	2	2	9	⚠️ 5台终端弱信号
行政区一楼	2台	15	15	29	✅ 正常
红枫大楼	2台	6	6	48	⚠️ AP-HF-OVERLOAD负载高，3台弱信号
TestAI场所	1台	1	1	3	✅ 正常
new	1台	0	0	0	🔴 **设备离线，需关注**
Changhe Road	1台	8	8	27	⚠️ 多处弱信号（-83dBm）
合计	**9台**	**32台**	**32台**	**116台**	

重点关注：

1. 🔴 **场所"new"** — 设备CAP-2离线，建议检查设备状态
2. ⚠️ **研发黄区** 下5台终端信号弱
3. ⚠️ **红枫大楼** AP-HF-OVERLOAD负载40台终端，建议关注性能
4. ⚠️ **Changhe Road** 多个AP下终端信号偏弱

输入 324818 输出 2353 共 327171 tokens 31.2s

智能排障：终端信号差故障定位

某园区有用户反馈发现笔记本接入无线后，无线信号差，视频卡顿。运维人员需要快速定位根因，但涉及有线、无线、广域网等领域，传统排查方式可能耗时几十分钟。

场景描述

对终端进行智能排障，确定根因并修复。

智能体
解决方案

第一阶段是无线信息收集：识别意图，启动无线终端排障skill。检查指定终端及关联AP信息，包括无线业务配置、无线射频状态（AP信道、同频干扰、发射功率等）。

第二阶段是数据验证与分析：多源数据自动交叉比对，按专家经验模型定位根因。如分析干扰占比、射频使用率、终端能力（802.11k/v/r 协议）、版本一致性。

第三阶段是关联分析与根因定位：智能体综合终端与网络情况，给出结论：终端粘滞，并给出3条建议：1. 建议下发一次Deauth引导，将终端踢下线，促使其重新扫描并关联到信号更好的邻居AP；2. 同时建议在AC上开启 802.11k/v 快速漫游协议（当前终端仅支持802.11v，不支持802.11k/r）；3. 可考虑配置 最小RSSI接入阈值。

第四阶段是故障修复：用户选择下发Deauth引导；智能体会让用户审批并确认下发的指令，确认后才会执行。

第五阶段是排障结果验证：在智能体执行操作后，用户检查终端当前信号情况，可以看到已连接到就近AP，信号变优秀。

红枫大楼[redacted]反馈信号不好，具体有什么问题



我先查一下这个终端的连接情况。

> getStationInfo 完成

该终端在红枫大楼（shopId:2897199）有连接记录，连接的AP序列号是[redacted]，AC是[redacted]（AC-HONGFENG），5GHz射频。先查AP详情和终端基本信息。

> getApBasicInfoDetail 完成

> getStaBasicInfoDetail 完成

终端连接的是 **AP-HF-WWK**（WA7220），5GHz射频。现在查看该AP射频下的终端信号分布和终端历史指标。

> listClient 完成

> getStaHistory 完成

> iserviceCheck 完成

查到了关键数据！现在让我进一步查一下弱信号历史

> getClientRssiLowProblemCount 完成

> getNbr 完成

弱信号历史高达 **633次**，远超3次阈值，说明这是个持续性弱信号问题。现在查终端过去7天是否连接过其他AP，以及邻居AP上的弱信号情况。

> getStationInfo 完成

该终端在红枫大楼只连接过 **AP-HF-WWK** 这一个AP，没有连接过其他邻居AP。邻居AP有 **AP-HF-NEIGHBOR**、**AP-HF-UPLINE-NB**、**AP-HF-3F-3**（同信道40/80MHz，SNR均为16dB）。现在查一下邻居AP上该终端的弱信号情况。

> getClientRssiLowProblemCount 完成

> getClientRssiLowProblemCount 完成

> getClientRssiLowProblemCount 完成

三个邻居AP上均无弱信号记录（0次），说明终端在邻居AP上信号正常，但一直粘滞在AP-HF-WWK上。现在查Deauth历史。

> clientDeauthHistory 完成

未下发过Deauth。根据技能流程，邻居AP上弱信号为0次，说明该终端可以关联更好的AP但没有主动切换，属于典型的**粘滞终端**问题。

📱 **终端信号诊断 — (李华)**

📊 **信号质量：**

- 接入AP：**AP-HF-WWK**（WA7220）— 5GHz / 802.11ac
- 当前信号强度：**-83dBm** 🔴 **差**（低于-75dBm阈值）
- 7天平均信号强度：**-83dBm**（持续差）
- 平均重传率：**0.41%** 🟢 优秀
- 平均时延：**19ms** 🟢 优秀
- 平均丢包率：**0.13%** 🟢 优秀
- 健康度评分：**91.58分** 🟢 良好

📋 **弱信号历史：633次** 🔴 高频次弱信号（持续性问题）

🔄 **排查路径：** 单终端场景 → 弱信号高频（633次>3）→ 邻居AP无弱信号→ 未下发Deauth

🔍 **诊断结果：**

该终端持续以 **-83dBm** 的弱信号连接 **AP-HF-WWK**，而该AP的三个邻居AP（AP-HF-NEIGHBOR、AP-HF-UPLINE-NB、AP-HF-3F-3）与AP-HF-WWK工作在同一信道（40/80MHz），且**终端在邻居AP上均无弱信号记录**（0次），说明终端本可以漫游到信号更好的AP，但未主动切换——这是典型的**粘滞终端（Sticky Client）**问题，即终端"粘"在弱信号AP上不主动切换。

💡 **优化建议：**

1. **建议下发一次Deauth引导**，将终端踢下线，促使其重新扫描并关联到信号更好的邻居AP
2. 同时建议在AC上开启 **802.11k/v** 快速漫游协议（当前终端仅支持802.11v，不支持802.11k/r），帮助终端及时感知更好信号并切换
3. 可考虑配置 **最小RSSI接入阈值**（建议-75dBm），低于阈值的终端不允许接入，从源头避免粘滞

需要我现在下发Deauth引导该终端切换AP吗?

输入 594335 输出 2663 共 596998 tokens 42.1s

执行建议1

好的，先执行Deauth，让终端重新漫游找更优的AP

resetClient 执行中

需要审批

AC序列号

终端MAC列表

✓ 批准原参数 修改并执行 × 拒绝

resetClient 完成

Deauth引导已成功下发！终端 （李华）已被踢下线，它将自动重新扫描周围的AP，预期会关联到信号更好的邻居AP（如AP-HF-NEIGHBOR、AP-HF-UPLINE-NB或AP-HF-3F-3）。

过一会儿可以让用户重新连接WiFi，信号质量应该会有明显改善。

输入 163168 · 输出 210 · 共 163378 tokens · 6.6s

检查下现在 的信号情况



getStationInfo 完成

已经在19:52左右重新上线了！而且切换到了新的AP，让我查一下当前实时信号。

listClient 完成

getStaBasicInfoDetail 完成

Deauth引导效果立竿见影！终端已成功切换到信号更好的AP，信号质量大幅提升：

终端0088-6778-3001 当前信号情况

指标	Deauth前	Deauth后 ✅	改善
接入AP	AP-HF-WWK	AP-HF-UPLINE-NB	切换成功
信号强度	-83dBm 🔴 差	-27dBm 🟢 优秀	提升56dB
协商速率	—	1233.4Mbps	大幅提升
IP地址	192.168.10.10	192.99.0.3	已更新

Deauth引导成功将终端从信号弱的 **AP-HF-WWK**（-83dBm）踢下线后，终端自动重新扫描并关联到了 **AP-HF-UPLINE-NB**，信号强度从 -83dBm 飙升至 **-27dBm**，达到优秀水平，协商速率也提升至 1233.4Mbps。李华的信号差问题已解决！

输入 250546 · 输出 622 · 共 251168 tokens · 12.9s

智能调优：无线射频调优

某企业园区有多个区域，传统方式使用人工分析流量报表和手动调整无线射频策略，响应滞后且容易误判。某天陆续有人反馈视频会议延迟高。



场景描述

智能体开启无线射频调优，建立从感知、分析到调优的完整自优化闭环。系统持续监控全网无线射频状态和业务流量，当检测到优化机会或异常时，自动触发射频优化。



智能体解决方案

第一阶段是感知当前无线射频状态：智能体分析无线射频数据，包括：网络配置、整体组网、无线射频现状、终端体验指标。

第二阶段是分析当前优化点：智能体发现存在2.4G频段拥塞，信道利用率高达62%；5G频段信道重叠，有同频干扰隐患；全网没有开启智能射频调优。

第三阶段是给出优化建议：综合网络整体信息，给出优化建议：建议开启RRM、信道调整。

第四阶段是用户审批与执行：用户下达开启RRM指令，智能体识别指令后提交用户审批，待用户确认后，执行开启RRM。

第五阶段是智能射频调优：基于AI算法持续监控关键指标，感知网络环境变化（如干扰、负载、终端粘滞），并自动调整AP的信道、功率和频宽，以持续优化无线网络性能。视频会议延迟从60ms降至20ms，无线终端RSSI均为优秀，优化目标全面达成。

检查下长河路7楼无线射频哪里可以优化



我来检查一下长河路7楼的无线射频情况。先查询场所列表找到这个场所

> listShop 完成

找到场所了，现在查询该场所的设备列表，找到AC设备

> listShopDevice 完成

有2台AC：YANFA7LOU-AC2 和 YANFA7LOU-AC3。先查一下射频详情，看整体射频数据

> listApRadioDetail 完成

我看到射频数据中有一个AP存在明显问题。让我进一步查看 **changhe7lou-AP2** 的射频历史数据，以及它的邻居情况，做更深入的分析。

> getApRadioHistory 完成

> getNbr 完成

现在让我再看看**changhe7lou-AP2**的详细信息和5GHz射频上的终端连接情况，以及AC的RRM配置

> listAp 完成

> getRRMSwitch 完成

现在让我看看所有AP的5GHz射频信道使用情况，特别是检查信道重叠问题

> listApRadioDetail 完成

现在我已经获取了足够的数据，综合分析如下：

长河路7楼 无线射频优化分析

📊 整体概览

该场所共有 **13台AP**（含2台AC：YANFA7LOU-AC2、YANFA7LOU-AC3），AP型号为 WA7320i 和 WA6620。

🔴 发现的主要问题

1. changhe7lou-AP2 — 2.4GHz射频严重拥塞（亟需优化）

指标	数值	说明
信道利用率(CCB)	62%	远高于正常阈值（<30%为健康）
信道空闲率(CFR)	仅38%	大部分时间信道被占用
干扰等级(CRB)	31%	接收信道利用率高，存在明显同频干扰
其他信道占用(COB)	31%	有非本AP发送的占用
AP评分	90分	已低于其他AP（均100分）
2.4GHz信道	信道6，20MHz	功率20dBm
2.4GHz终端数	0	当前无终端连接，但信道被大量占用

分析：AP2的2.4GHz射频存在**严重的同频干扰**，信道利用率高达62%，其中接收干扰(CRB)占31%，其他干扰(COB)占31%，发送利用率(CTB)为0%。这说明该射频的信道被**外部邻居AP或非管理AP**严重占用，属于典型的**同频干扰/假拥塞**问题。

2. 5GHz射频全局信道重叠严重

所有13台AP的5GHz射频全部使用信道40，80MHz频宽，功率均为20dBm。这意味着：

- 所有AP的5GHz射频工作在**完全相同的信道（40）**，且**80MHz大频宽**覆盖范围广
- 密集部署环境下，相邻AP之间的同频干扰会非常严重
- RRM（射频资源管理）**当前处于关闭状态**，无法自动优化信道分配

3. changhe7lou-AP2 5GHz射频负载偏高

5GHz射频当前关联**12台终端**，是场所内终端数最多的AP之一（与AP-拐角并列），存在一定负载压力。

✅ 优化建议

建议一：开启RRM（射频资源管理）

RRM当前为**关闭状态**。开启后系统会自动优化信道和功率分配，避免AP间同频干扰。

> *可通过 `setRRMSwitch` 开启，将14台AP的5GHz信道分散到不同信道（如36、40、44、48、149、153等）*

建议二：AP2 2.4GHz射频信道调整

当前2.4GHz全场所都使用**信道6**，AP2的2.4GHz干扰最严重。建议：

- 将AP2的2.4GHz切换到**非重叠信道**（如信道1或11），避开干扰源

建议三：AP2 5GHz负载分流

AP2的5GHz射频挂了12台终端，建议检查是否有终端可以引导到其他AP（如AP1、AP3），均衡负载。

建议四：降低部分AP的5GHz功率

当前所有AP的5GHz功率统一为**20dBm**。对于部署密集的区域（如办公区多个AP），适当降低功率（如15-17dBm）可减少同频重叠覆盖范围，降低干扰。

总结：首要优化动作是**开启RRM**，让系统自动分配信道和功率，解决当前所有AP5GHz挤在信道40的问题。其次是**调整AP2的2.4GHz信道**，解决其射频拥塞问题。

需要我帮你执行RRM开启或信道调整操作吗？

输入 320615 · 输出 1672 · 共 322287 tokens · 30.1s

RRM开启



好的，我来开启RRM。需要场所名称作为参数，场所名称为"长河路7楼"。

setRRMSwitch 执行中

需要审批

场所名	长河路7楼
设置状态	开启

✓ 批准 × 拒绝

好的，我来开启RRM自动调优功能

setRRMSwitch 完成

RRM自动调优已成功开启！系统会自动进行以下优化：

1. **自动信道规划** — 各AP的5GHz会从当前全部挤在信道40，自动分散到不同信道，消除同频干扰
2. **自动功率调整** — 根据AP覆盖情况和终端分布，自动调整各AP的发射功率，实现负载均衡
3. **持续动态优化** — RRM会持续监测射频环境变化，实时调整信道和功率配置

开启后，原来突出的几个问题（5GHz全信道40同频问题、AP-guaijiao负载过重、AP2 2.4GHz干扰）都会由系统自动逐步优化调整，无需手动干预。

输入 143587 · 输出 244 · 共 143831 tokens · 7.3s

新华三网络智能体架构

整体架构

新华三网络智能体，通过融合 AI 原生网络能力和智能体编排能力，以“自然语言对话”方式为客户提供“知识问答、态势查询、智能排障和网络优化”服务，重塑客户网络运维体验。基于开放Skills技能库和MCP标准接口，赋能第三方智能体具备专业网络运维能力。

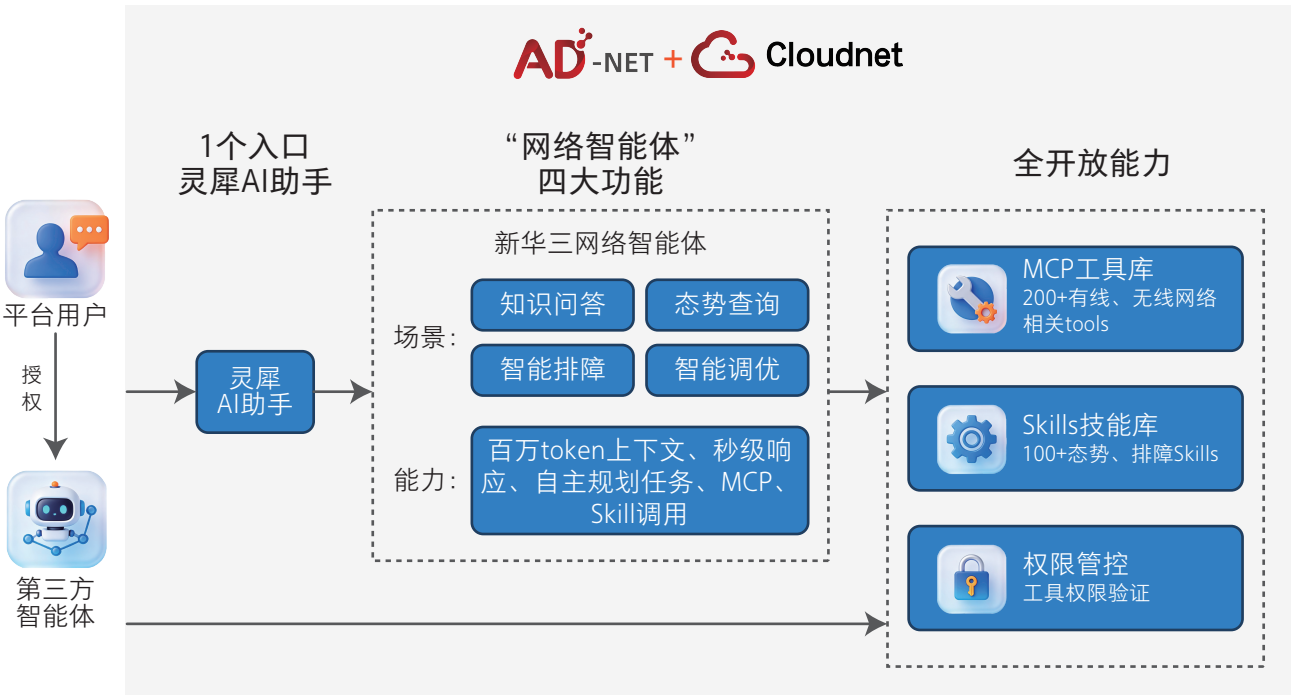


图1 网络智能体整体架构

网络智能体业务规划双引擎

“Skill+ReAct” 双引擎架构，通过“固定技能 + 动态推理”组合模式，高频场景靠 Skill 保障执行效率，长尾场景由 ReAct 覆盖复杂、个性化需求，实现了“确定性场景提效、探索性场景兜底”的全面覆盖。

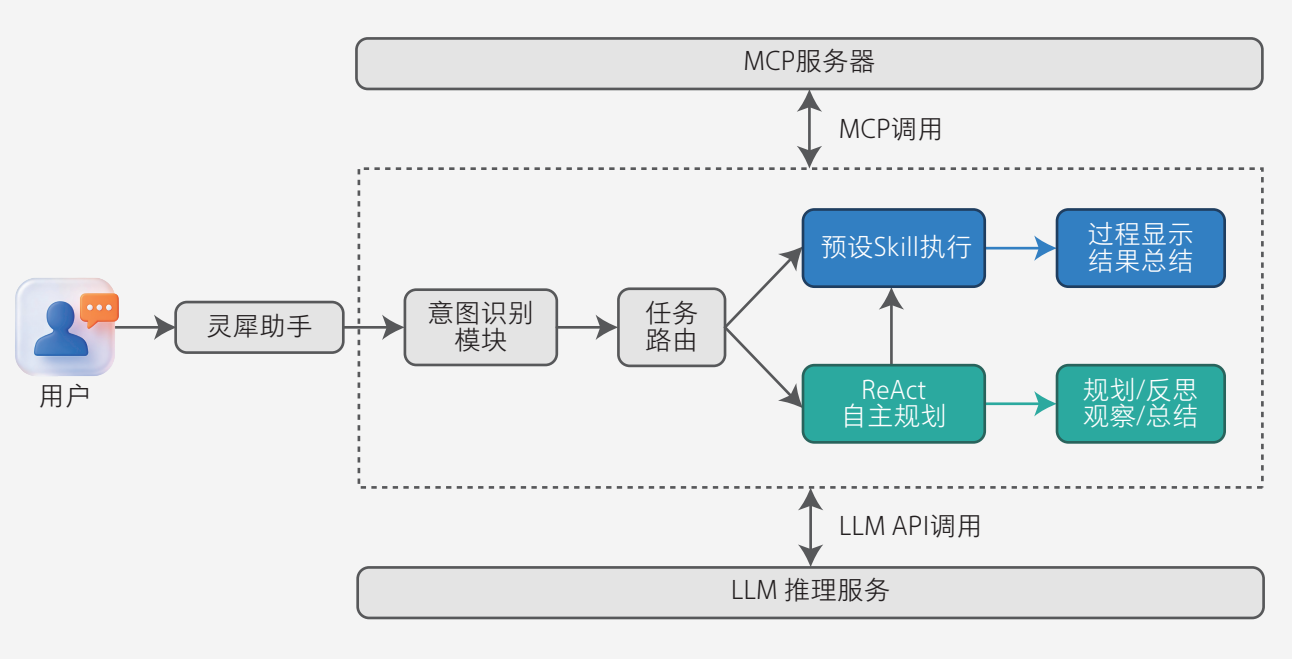
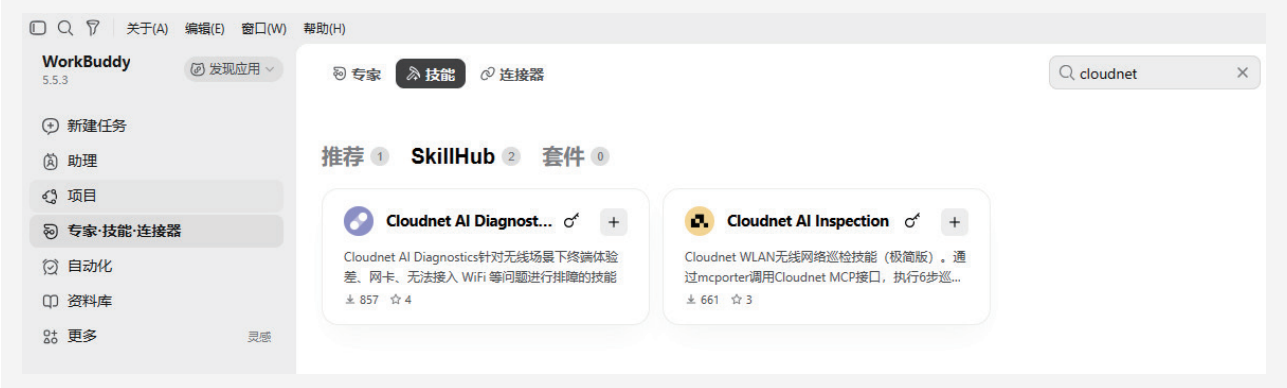


图2 业务规划双引擎

支持客户自有智能体

新华三Cloudnet已在Clawhub、腾讯Skillhub等平台发布相关skill，客户可以通过自有智能体使用Cloudnet发布的skill、MCP，执行巡检、排障、态势查询等。

例如，在 WorkBuddy 技能中搜索 Cloudnet，可以看到已发布skill；在连接器页面，可以找到灵犀助手。





使用这些skill/连接器/MCP, 需要提供认证KEY; 认证KEY在登录Cloudnet后, 在网络管理—>设置—>开放平台中找到。此KEY切勿对外泄露。



在配置完后，可在智能体中进行问答。例如，配置完连接器后，提问“Cloudnet 中有哪些设备掉线”，即可查看自己场所中设备离线情况。

cloudnet中有哪些设备掉线

WorkBuddy

已完成 1m38s >

查询完成。Cloudnet 当前共纳管 **15 台设备**，**10 台掉线（离线）**，**5 台在线**，掉线率约 66.7%。

掉线设备清单（status=0）

设备名称	序列号	类型	型号	所属场所	管理 IP
219801	21980	交换机	S5024PV5-EI-HPWR	switch	22
AP1	21980	云AP	WA6338	test-license	39
F1000-C8320	21980	防火墙	F1000-C8320	TEST312	22
SWITCH(0019)	21023	交换机	S6520-30SG-SI	TEST312	22
G-AC1	21023	AC	WBC580G2-BASE	TEST315	22
SWITCH(01PR)	21980	交换机	S5130V2-28P-HPWR-SI	testzj	39
AC	21980	AC	WX2560X	testzj	39
AC-CHANGHE	21023	AC	WX5580H	长河11楼	22
N-AC1	21023	AC	WX5540H	总部场所	22
TR-AC12	21023	AC	WBC580G2-BASE	总部场所	22

几个值得注意的点

- **类型分布**：掉线的 10 台里 **AC 占 5 台**（G-AC1、AC、AC-CHANGHE、N-AC1、TR-AC12），交换机 3 台，云AP、防火墙各 1 台。AC 是无线业务的控制器，掉线会直接影响其下 AP/终端。
- **疑似共因**：10 台中有 **8 台的管理 IP 都是 `221.12.4.143`**（另一组 `39.144.130.x` 也有 2 台掉线），集中在同一出口 IP 下批量离线，很可能是该上联链路/管理通道故障，而非设备各自独立掉线。
- **仍在线**：B11-Virtual (WSG1840X)、B11-WS (WX2560X)、onu (S3210-8P)、yyy (S5130V2-52S-SI)、行政11-B4 (WSG) 这 5 台正常。

需要的话，我可以针对掉线设备做进一步排查——比如逐个调用 `getDeviceRunInfo` 看运行信息，或对特定场所用 `getShopNetworkProblem` / `getProblemDistribute` 拉取掉线根因和告警。要我针对哪台或哪类设备深入查吗？

展示详情 ···



H3C网络智能体部署

公有云部署

Cloudnet部署在云端，网络智能体整体云上部署。用户可以直接使用已部署完成的网络智能体。

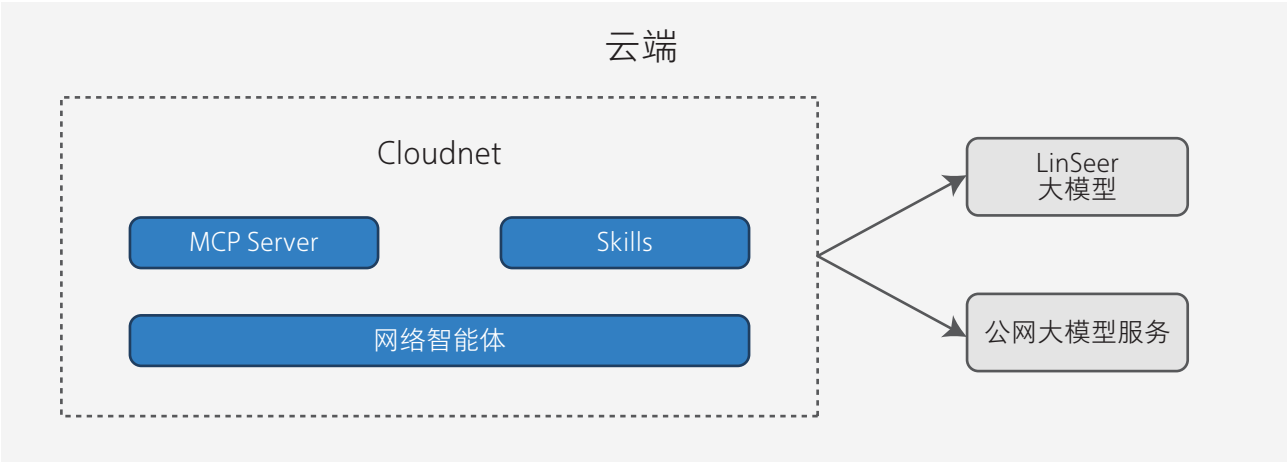


图3 云端部署方式

本地部署

AD-Net和使能平台部署在本地，二者双向互通，网络智能体Workflow和知识图谱部署在使能平台。支撑网络智能体的MCP Server、Skills部署在AD-Net端。

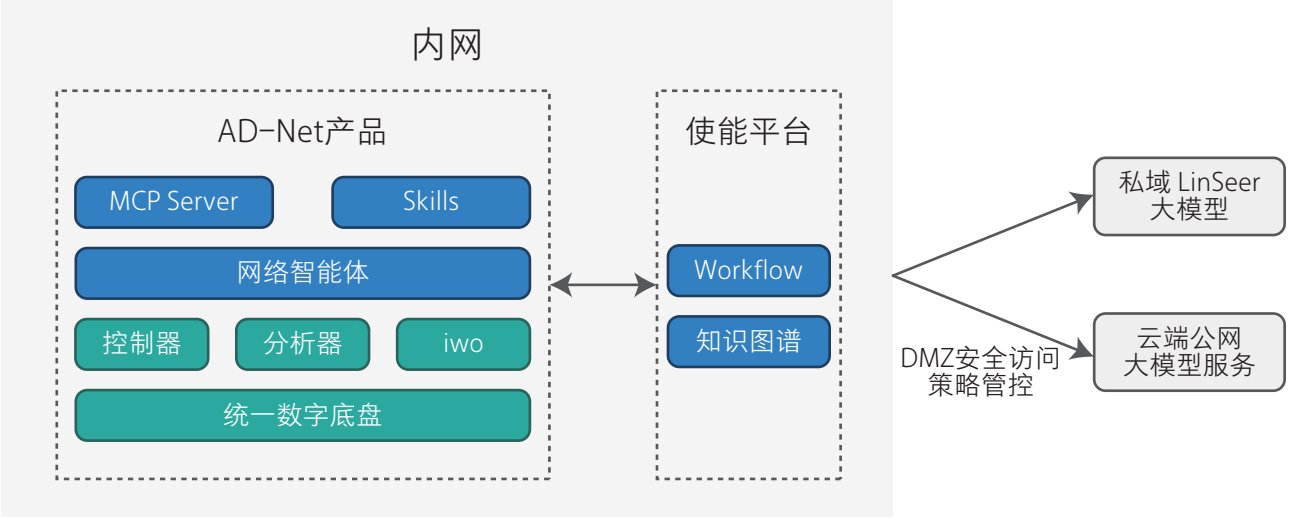


图4 内网部署方式

网络智能体未来蓝图

展望未来，网络智能体技术将沿着协作化、自主化和进化化的方向持续演进，最终构建人机协同、智能自治的下一代网络管理体系。

多智能体协同

未来网管系统将由大量专业智能体构成开放协作生态：各智能体聚焦路由、安全、无线、云等特定领域，通过 A2A 协议跨域协作。面对跨域复杂问题，系统自动组建"虚拟专家团队"会诊决策；协作还可突破组织边界——设备厂商、云服务商与企业智能体在同一安全框架下协作，形成端到端诊断能力。例如混合网络出现连通性故障时，三方协同可自动定位问题在云侧 VPC、专线接入还是企业侧策略，大幅缩短跨域排障时间。

原生智能的网络设备

网络设备将从被管对象进化为自主智能的 Agentic Device: 内置 AI 推理芯片与语言模型，通过设备内 MCP Server 暴露管理接口，支持自然语言交互，并可主动上报状态。其三大核心能力为——自诊断: 实时分析运行状态，预判故障并提前上报; 自优化: 按流量模式与应用需求自动调整转发策略与资源分配; 自适应: 随网络环境自动调参（如动态调整 ECN 阈值与队列调度策略）。设备由此从"等待被管理"转向"主动参与管理"。

人机审核与自我进化

未来的智能体系统将建立持续进化的能力，通过与人类的交互不断学习和成长。每次人机交互都是一次学习机会: 运维人员的追问揭示了智能体回答的不足之处，运维人员的纠正提供了准确的监督信号，运维人员的赞许确认了正确的行为模式。这些反馈被系统收集和分析，用于持续优化智能体的知识库、推理策略和交互方式，并保证进化过程可控。

自我进化还体现在知识的自动更新上。当网络环境发生变化（如新设备上线、新协议部署、新策略生效）时，系统自动更新知识图谱和相关Skills。当新的故障模式出现时，系统自动从排障过程中学习并将其纳入诊断知识库。随着时间推移，智能体系统的专业能力和决策质量将持续提升，逐步接近甚至超越资深人类专家的水平。

智能体时代的网络软件架构正在重新定义网络管理的范式。从REST到MCP、从传统消息到A2A、从Workflow到Skills、从GUI到Canvas，每一次变革都在推动网管系统向着更智能、更自主、更协作的方向演进。记忆、知识、护栏和委派的工程优化为智能体的可靠落地提供了坚实基础。知识问答、态势查询、智能排障和网络优化的最佳实践证明了这一架构的实战价值。基于Canvas的多人协同、多智能体生态、原生智能设备和人机协同进化，构成了网络运维的美好未来。

编委（按姓氏拼音首字母排序）：
丁伟　龚大富　刘浩　夏青　张俊　赵昌峰　钟果

Cloudnet
（扫码后，选择访客登录
进入演示场所
点击右下角灵犀AI助手
即可开启体验）

新华三网络
微信公众号

让每一张网络
都有AI专家相伴