**面向传统网络的分布式故障与异常分析系统：核心需求列表**

**第一部分：分布式边缘节点（硬件探针）核心能力**

此部分定义了部署在网络关键节点上的独立硬件设备（盒子）所需具备的核心功能，强调数据采集的保真度与边缘处理的效率。

1. **高性能全流量采集与存储**

* **线速捕获**: 支持在高速链路（例如10G/40G/100G）上无丢包地进行全流量数据包（Full Packet Capture）的实时捕获 (1)。
* **大容量本地存储**: 内置高容量、高读写性能的存储介质，能够将原始数据包在本地进行长时间（数天至数周）的完整留存，为深度故障追溯提供无可辩驳的原始证据 (2)。
* **高可靠性**: 硬件设计应具备高稳定性，支持旁路部署（通过TAP/端口镜像），确保不影响主干网络的正常运行 (3)。

1. **边缘实时数据预处理与指标提取**

* **深度协议解码**: 具备强大的协议解析能力，能实时解码数百种网络协议和主流应用协议 (1)。
* **关键性能指标（KPI）提取**: 在捕获流量的同时，实时计算并提取超过200项关键性能与故障指标，如网络时延、服务器响应时延、TCP重传、丢包率、应用交易成功率等，并将这些轻量化的指标数据发送至中心平台 (2)。
* **元数据生成**: 生成会话、数据流、日志等结构化的元数据，为中心的快速检索和大数据分析提供基础 (2)。

**第二部分：中心管理与分析平台核心能力**

此部分定义了中心平台的功能，强调对分布式节点的统一管控、全局态势的可视化以及实时分析能力。

1. **分布式节点统一管控**

* **集中配置与管理**: 能够对全网所有分布式硬件探针进行统一的策略下发、状态监控、版本升级和远程维护 (3)。
* **数据汇聚与查询**: 集中汇聚所有边缘节点上传的KPI指标和元数据，并提供统一的查询入口 (4)。
* **按需数据回溯**: 当需要深度分析时，允许管理员从中心平台发起请求，快速检索并调取存储在任意边缘节点上的特定历史时段的原始数据包 (2)。

1. **网络全局态势可视化**

* **自动化网络拓扑发现**: 能够自动发现网络中的设备和链路，并生成动态、可交互的全局网络拓扑图，直观展示网络结构 (5)。
* **多维度性能仪表盘**: 提供可定制的仪表盘，通过图形、图表等方式，从全局、区域、链路、应用等多个维度实时展示网络健康状况和关键性能指标 (4)。
* **链路健康度监控**: 实时监控关键链路的带宽利用率、流量组成、延迟、抖动和丢包情况，快速识别拥塞或质量下降的链路 (6)。

**第三部分：AI驱动的智能故障定性与根因分析**

这是解决方案的核心竞争力所在，强调利用AI/机器学习能力，将海量数据转化为可操作的、精准的故障洞察，实现从“告警”到“答案”的转变。

1. **动态基线与智能异常检测**

* **自适应基线学习**: 系统能自动学习网络中各项指标（如流量、时延、应用交易量）在不同时间（如工作日、节假日）的正常行为模式，形成动态的、多周期的性能基线 (7)。
* **多维异常检测**: 基于机器学习算法，而非简单的静态阈值，对偏离正常基线的行为进行检测，能够发现包括突刺、整体抬升/下降、周期性失效等复杂模式的异常 (9)。

1. **智能告警降噪与事件关联**

* **告警风暴抑制**: 当一个底层故障（如核心交换机故障）引发大量相关告警时，AI引擎能够自动将这些告警聚合成一个根本性事件，大幅减少告警噪音，帮助运维人员聚焦核心问题 (11)。
* **跨域事件关联**: 能够分析不同节点、不同指标之间的因果关系，将看似孤立的异常现象（如A应用的响应变慢和B数据库的CPU升高）关联起来，构建故障传播链 (11)。

1. **自动化故障诊断与定性**

* **内置专家诊断模型**: 将常见的网络故障排查逻辑（如MTU不匹配、TCP连接慢、设备延迟、DNS解析慢、负载均衡配置错误等）模型化，系统可自动进行匹配诊断，并给出明确的定性结论 (14)。
* **根因推荐**: 在识别故障后，系统能自动分析并推荐最可能的根本原因，并按可能性进行排序，极大地缩短人工排查时间 (15)。
* **引导式排错建议**: 针对已定位的故障，系统能提供清晰、可操作的修复建议或下一步排查指引，赋能初级运维人员处理复杂问题 (12)。