



向自动化世代跃迁

构建更智能的自治型网络

白皮书
向自动化世代跃迁:构建更智能的自治型网络

Alcatel·Lucent 
Enterprise

介绍

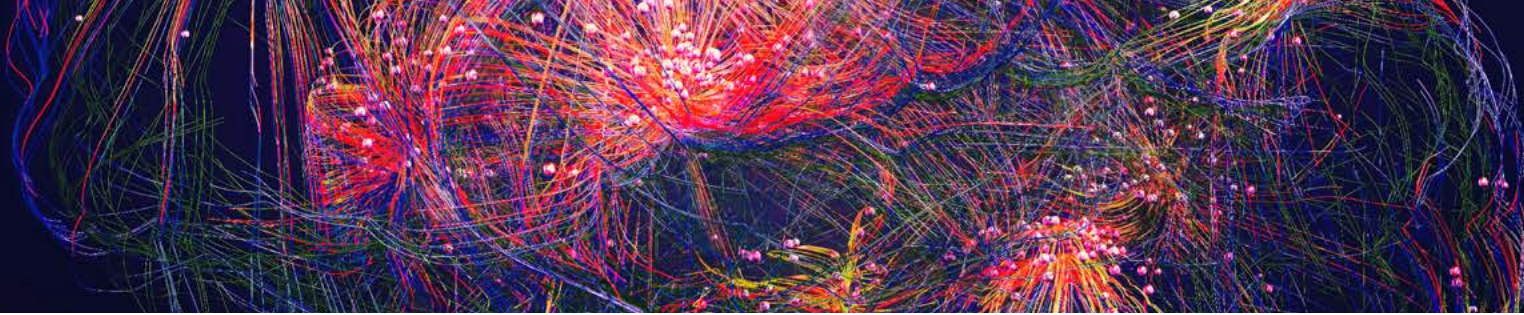
在当今的数字化时代,随着云计算的快速普及、物联网设备的广泛部署和日益恶化的网络安全威胁,企业网络架构正在变得越来越复杂。依靠人工主导的网络管理模式已难以为继,传统的运维方法已无法匹配现代业务运营的节奏和需求。

本白皮书深度探讨了网络架构从传统自动化向“自治型网络”演进的历史进程,并着重阐述了人工智能(AI)与机器学习(ML)在其中发挥的关键作用。自治型网络能够对网络性能执行实时、持续的监控、分析与优化,在最大限度消除人为干预的同时,为企业提供了高可靠的解决方案。

本白皮书展示了一系列经过商业验证的AI驱动用例,这些实践有效化解了传统自动化机制难以攻克的关键网络运维挑战,并展示了网络智能的发展轨迹:从故障发生后才被动介入的“被动响应式AI(Reactive AI)”,全面跨越至能够在问题波及业务前进行预判与阻断的“主动预防式AI(Proactive and preventive AI)”。这一演进的终极形态将是“决策指导式AI(Prescriptive AI)”——即智能系统基于深度数据挖掘提供高阶建议,辅助企业制定战略决策。

通过将自动化架构与AI战略深度融合,企业能够确保网络运营的可靠与高效,在当今错综复杂的IT生态中保持高稳定性、可自愈性和竞争优势。





理解自治型网络

自治型网络本质上是一个高度自运行的系统架构。它能够严格映射并遵循顶层业务目标进行运转,除系统初始阶段的人工输入(即以业务意图、宏观目标、控制策略或特定配置数据等形式)之外,全程无需任何人为干预。其核心设计理念是通过一系列闭环的自动化操作实现网络的内生管理,具体涵盖六大能力维度:自配置、自诊断、自修复、自治愈、自优化与自保护。自治型网络能够从海量数据中自动发现运营态势并自主触发执行动作,这为上述“六自”能力的全面落地奠定了底层基础。

自治型网络具备以下关键特性:

- **感知能力** - 持续监控自身运行环境、性能及内部状态,判断是否符合预定义且已达成共识的目标。
- **自适应能力** - 能动态调整运营方式,以适应短期和长期内的环境变化,包括修改决策与行为,确保运营性能的持续性。
- **自动化能力** - 可独立控制内部资源与运营流程,无需人工干预即可正常运行。

网络的“能力水平”存在差异,涵盖从基础自动化到完全自治的不同阶段。

自动化和自治型的区别

网络自动化与自治型网络是两个常被混淆的概念。但二者在技术路径、系统功能涵盖面以及人工干预边界上存在着显著差异。

网络自动化侧重于利用软件工具和既定流程,以编程化脚本的方式管理网络基础设施与服务。其核心价值在于将参数配置、业务部署和巡检维护等高度重复性任务转化为自动执行,从而提升运维交付效率并规避人为操作失误。然而,在自动化模式下,决策制定与规则设定的最高控制权依然高度依赖人工介入。系统仅被局限在预先设定的参数和条件框架内运转。在此阶段,生成式 AI 主要作为辅助工具,用于简化网络管理员与复杂系统之间的交互指令输入。

相比之下,自治型网络代表了一种具备自我管理能力的网络架构。它深度融合了人工智能/机器学习,旨在最大限度地减少甚至彻底消除人为干预。自治型网络能够原生地完成自配置、自监控、自维护与自安全防护。其核心差异特征在于“系统主导决策”,人类角色被完全移出常规控制闭环,仅在必要时履行最高层级的安全与监督职能。当然,迈向完全自治型网络是一个渐进过程。在企业网络架构师完全移交网络控制权之前,系统必须逐步提升,利用自治水平,以长期无故障运行的数据表现来持续积累建立“系统级信任度”。

两种概念针对不同的网络管理场景:自动化网络适用于已知的重复性问题,管理员需投入时间和精力开发技术方案来解决这些问题;自治型网络则针对罕见且通常未知的问题,这类问题可通过人工智能/机器学习方法识别。二者结合,为网络的良好运行奠定了坚实基础。

基于自动化的网络管理

自动化的本质是实现任务的无人工干预执行。这一目标可通过引入自动化功能,或利用自动化工具(如执行一系列命令的脚本)增强、重构甚至完全替代传统的人工作业流程。

自动化的应用分类各不相同,既可以针对单个任务和流程,也可以覆盖基础设施的完整管理与运营(涵盖网络和服务的整个生命周期,包括安装、配置、资源分配和终止)。控制平面与数据平面的解耦、虚拟化技术等创新可进一步增强自动化能力,提升灵活性。然而,关键挑战在于如何将这些可组合组件整合为统一、高性能、稳健、可扩展且可重构的自动化系统,这增强了对标准化接口、模型和机制的需求。

开发完全集成的自动化解决方案仍是一项复杂且尚未解决的挑战。此类解决方案需要对具备以下特征的自动化功能进行无缝编排:

- 纵向端到端自动化,覆盖从服务层到物理层的整个协议栈。
- 横向端到端自动化,涵盖多种技术和管理域。
- 可重复性与可复用性,利用标准化接口和最佳实践,确保广泛适用性。
- 控制权限的动态可配置性。

此外,明确自动化是由技术策略驱动还是业务意图驱动,也至关重要。单一技术骨干将实现对所有环节的管理。

借助这一集成架构,智慧楼宇 5.0 将通过多个传感器管理室内温度、照明和窗帘控制。利用其真正的智能架构,楼宇可对数据进行收集、分析、报告,并自主根据所有可用信息采取行动以支持持续运营;同时,楼宇还能基于室内外环境数据预测所需的运行参数调整,并根据这些预测采取行动,以实现再生建筑的目标。

基于策略的自动化

自动化操作通常可由策略管控。目前,许多网络部署已融入动态策略管理,能够在生命周期管理和其他网络配置中实现自动化调整。

基于策略的自动化,其核心是当满足特定条件时,触发相应操作的预定义规则。这些条件包括:

- 基于时间的触发条件(如一天中的特定时段、一周中的特定日期等)
- 网络负载阈值
- 系统发生故障
- 上述条件的组合

当触发条件发生时,本地管理实体将执行预定义操作,例如:

- 部署或终止服务 / 组件
- 资源扩容
- 工作负载迁移
- 实例替换
- 配置调整
- 软件更新管理

策略部署完成后,基于策略的自动化可实现完全自治的零接触管理。但如何制定策略,并使其随环境变化动态调整,仍是一项复杂挑战。而引入高层级的业务导向意图,可在一定程度上改善这一状况。



基于意图的自动化

基于意图的自动化以基于意图的网络 (IBN) 为基础, 它利用智能软件理解用户目标, 并自动将其转化为具体的服务或网络配置。由于 IBN 是一种相对较新的机制, 其定义尚未统一, 目前也不存在标准化框架。

IBN 是继基于策略的自动化之后, 网络管理的下一阶段发展方向。策略定义的是具体的决策规则, 而意图代表的是更高级别的声明式目标。基于意图的 API 允许用户指定期望结果, 低层级系统则会动态确定最优的网络设置。

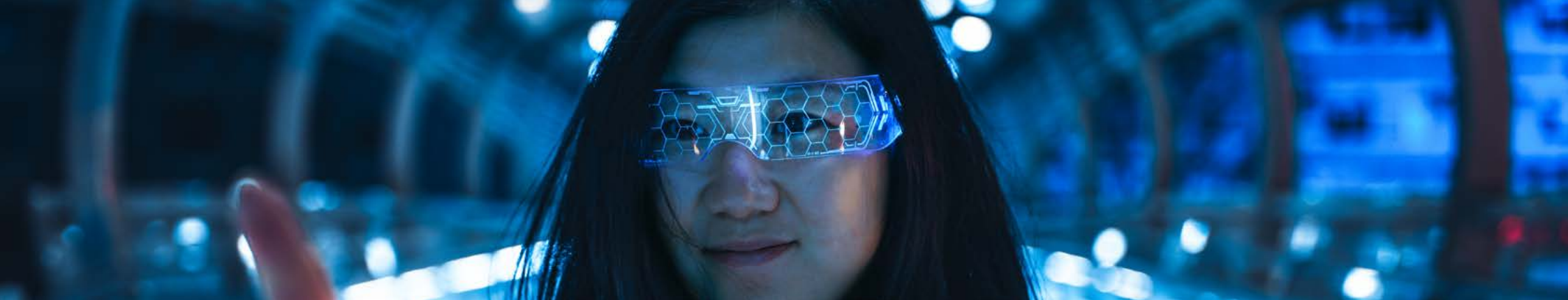
传统管理系统在服务需求变化时, 需要修改配置, 而真正的意图驱动的方法依赖语义模型, 可实现基于行为的自动化, 无需手动调整配置。与策略不同, 意图不会因基础设施变化或故障而改变, 这使得管理应用不需要关注网络特定细节, 从而简化服务的开发、测试和部署流程。

依托高可扩展的意图 API 标准, 独立开发运营的各类第三方应用服务能够使用同一种通用标准化规范语言来明确其对底层计算与网络资源的诉求。对于当今深度耦合了 SDN 架

构、SD-WAN 多云互联、MPLS 专线网络、混合云 (公有云/私有云) 集群以及分布式边缘计算 (Edge computing) 节点的异构现代 IT 生态而言, 至关重要。

生成式人工智能可以弥合高层级业务意图与低层级网络配置之间的差距。它通过解读用户输入的自然语言, 将其转化为可执行的技术策略。例如, 若用户提出“优先处理视频会议流量”的目标, 生成式人工智能可确定实现该意图所需的服务质量 (QoS) 设置。它利用基于网络数据和策略规则训练的模型, 确保转化的准确性和相关性, 从而使非技术相关人员无需理解复杂的配置语法, 即可表达业务目标。

此外, 生成式人工智能还会考虑网络环境的背景 (如现有策略、性能指标和合规要求), 以避免冲突并确保新配置与整体网络战略保持一致。随着时间推移, 生成式人工智能可从用户反馈和网络行为中学习, 不断提升策略生成能力, 使网络管理更直观、更敏捷, 并与业务目标高度契合。



三擎驱动的 AI 网络演进路线图

当前,在重塑下一代自治型网络管理模式的进程中,存在三种占据核心主导地位的 AI 技术路线,分别是预测性人工智能、生成式人工智能和智能体人工智能。

预测性人工智能

预测性人工智能利用历史数据、统计模型和机器学习算法预测未来结果或行为,通过识别模式和趋势做出有依据的预测(如预测系统故障或性能下降)。其核心应用场景包括:

预测性人工智能的关键应用包括:

- **异常检测的动态阈值:**与静态、预配置的阈值不同,基于机器学习的阈值会根据不断变化的模式和趋势实时调整,实现更具适应性和响应性的监控,进而提升异常检测效率。
- **自动化事件关联:**人工智能可识别事件之间的隐藏关联,为高效的根本原因分析提供支持,显著缩短事件响应时间并减少人工操作。
- **智能日志分析:**人工智能能利用历史数据对新增及罕见的系统日志消息进行分类和解读,无需预定义解析规则即可识别关键事件。

生成式人工智能

生成式人工智能通过应用大型语言模型(LLM)从数据中学习模式,进而生成新内容。其关键应用包括:

- **自适应报告:**人工智能根据当前网络状况生成实时、上下文感知的报告,确保相关洞察随时可用。
- **管理员自然语言界面:**人工智能可将自然语言命令转换为网络配置或查询指令,还能通过对话式提示实现与网络数据的直观交互。

白皮书

向自动化世代跃迁:构建更智能的自治型网络

智能体人工智能

智能体人工智能利用高级逻辑,代表用户做出决策并采取行动,它整合了预测性模型和生成式模型,通过多步骤推理和自适应学习展现目标导向行为,并借助实时反馈循环(评估结果并据此调整)持续优化性能。

智能体人工智能的核心应用是智能工作流:网络工程师将一系列网络管理任务委托给人工智能智能体,智能体自主确定完成请求的方式(通常涉及与多个系统的交互,包括收集数据、执行后续查询和解读结果);流程完成后,人工智能智能体向工程师提供全面的响应。

基于自治的网络管理

传统网络自动化主要侧重于简化高频或关键任务,例如:

- 对常见的系统日志消息应用解析规则
- 当关键指标超过预定义阈值时生成告警
- 根据典型模式或重复组合关联事件

然而,这种方法忽略了大量定义不够明确但可能至关重要的任务。要解决这些任务,需要采用完全不同的策略——即利用人工智能和机器学习的能力。即便在未针对每个场景明确定义规则的情况下,这些技术仍能实现自动化与优化。

上述三类人工智能,结合自动化方法及其他技术,共同构成了网络自治的核心驱动力:闭环自动化。

闭环自动化是一种系统持续收集数据、分析数据、制定和应用配置决策并迭代此循环以根据先前操作的反馈改进结果的方法。

网络从手动操作向完全自治演进的过程中,会经历多个阶段,如辅助自动化、部分自动化、条件自动化、高度自动化和完全自动化。在更高层级,闭环自动化会变得更加复杂,能够实现自愈、自优化和主动问题解决。

闭环自动化主要包括四个阶段:监控、分析、决策和执行。

监控阶段:数据收集与摄取

监控阶段负责从网络设备收集数据并进行预处理——即“数据摄取”,具体是将数据从一个或多个来源传输到中央存储库,用于后续存储和分析。收集的数据形式多样,包括事件、日志、遥测数据和流量捕获数据等。

分析阶段:提取洞察

分析阶段从监控阶段收集的实时数据、历史记录、网络配置以及描述网络的知识库信息中提取洞察。这些洞察可回答以下关键问题:

- “发生了什么?”:检测异常或异常网络行为
- “为什么会发生?”:通过根本原因分析确定潜在问题

洞察生成是一个持续过程,会通过监控阶段新传入的数据不断完善。

决策阶段:确定行动方案

决策阶段将洞察转化为指导系统响应的工作流,并根据检测到的问题确定相应行动方案,具体包括三种类型:

- **被动响应式**:在问题发生时进行处理
- **主动预防式**:根据检测到的“问题发生前通常出现的数据模式”,预防潜在问题
- **预测式**:基于数据趋势预判未来可能出现的网络问题

决策阶段利用人工智能/机器学习、规则和策略,将发现的洞察转化为行动清单,引导网络走向最优状态。

执行阶段:实施操作

执行阶段负责执行决策阶段确定的工作流,对网络进行纠正性或适应性操作。这些工作流由一个或多个操作组成,需精心编排以确保无缝实施。数据建模模型,如 YANG 模型,以及相关协议,如 NETCONF 和 RESTCONF,是这一阶段的重要组成部分。

工作流执行完成后,闭环自动化逻辑会启动新的“监控 - 分析 - 决策 - 执行”循环,同时考虑前一周期操作的结果以及新的外部网络条件。



结论

向自治型网络转型,是企业提升运营效率、敏捷性和用户满意度的关键一步。传统网络自动化已带来显著效益,如减少人工工作量、降低人为错误、加快常规操作速度;而在此基础上,闭环自动化进一步实现了对网络状况的实时监控和自动响应,确保更快的问题解决速度和更高的可靠性。此外,闭环自动化还能通过从网络行为中学习,并在无需人工干预的情况下调整,实现持续优化。最终,自治型网络为企业赋予了自我管理、自愈和自优化能力,在降低运营成本的同时,提升了网络的可扩展性和韧性。在日益复杂的网络环境中,拥抱这一演进趋势,是企业保持敏捷性和竞争力的关键。