CAICT 中国信通院

集智 专题报告

万兆 AI 园区网络以太技术研究报告

中国信息通信研究院技术与标准研究所

2026年7月

版权声明

前　言

随着行业数智化转型的持续深入以及人工智能（AI）的迅猛发展，园区网络的业务模型与运行范式正迎来新一轮的演进升级。一方面，AI Agent 的爆发式增长和多模态交互普及推动数据量呈指数级增长，对园区网络的超宽承载能力与无线接入性能提出了更高要求；另一方面，传统园区“烟囱式”建网模式导致数据孤岛严重、建设成本攀升、数据价值难以释放，无法匹配 AI 时代数据融合的发展需求。同时，各类智能终端、异构物联设备大规模接入园区网络，传统边界防御、外挂式安全体系防护能力不足，难以应对新型网络风险；人工主导的运维模式，也无法满足 AI 时代网络实时感知、快速自愈的业务诉求。为此，构建面向智能时代的万兆 AI 园区网络，成为推动园区数智化转型升级的必然路径。

本报告结合智能时代的技术应用，深入分析当前园区网络业务的发展趋势，客观剖析园区网络面临的难点与挑战。结合行业园区网络主流建网技术，对基于以太网架构的万兆 AI 园区网络技术进行了研究，系统阐述了万兆接入、无线融合、全域安全、网络自智四大核心特征及对应的关键技术；并结合教育、电子政务、金融、医疗、工业制造、酒店、零售七大重点行业的典型应用案例，全面展现万兆 AI 园区网络关键技术在不同业务场景下的落地模式与应用成效。以期为产业界和技术决策提供系统性参考，助力万兆 AI 园区网络的标准化建设与规模化部署，推动园区网络基础设施与 AI 业务深度融合，赋能千行百业的高质量发展与数智化升级。

目 录

图 目 录

表 目 录

一、园区业务发展趋势

当前企业业务正处于从信息化向智能化跃迁的关键拐点：日常办公应用的角色正由“辅助人完成任务的工具”转变为“可自主执行任务的智能体”，工作组织方式、流程、人机分工都将被重新定义。随着大模型推理能力的质变与成本指数级的下降，未来五年 AI 将成为企业办公的主体——应用从“嵌入助手的工具”进化为“自主执行的智能体”，员工工作模式从“亲自操作系统”转向“指挥和治理智能体完成工作”。伴随着 AI Agent 规模化落地，企业园区网络也将会随之发生巨大的变化。具体总结为以下四个趋势：

趋势一：AI 应用改变企业办公业务交互模式。据 Gartner 预测，2026 年预计将有 40%企业应用嵌入 Agent 来处理日常任务，较 2025 年的不足 5%实现跨越式增长。随着 OpenClaw、Hermes 等 Agent 框架日趋成熟，端侧 Agent 已可跨应用、跨平台处理复杂业务流；同时大模型的多模态能力普及，交互从单一模态例如文本向多模态如语音、图像、视频等演进。单个 AI Agent 上行带宽峰值可达 10–20Mbps，复杂多模态场景可突破 100Mbps，相比过去以音视频为主的 2–4Mbps 办公流量增长 5 倍以上。更关键的是，端侧 Agent 数量将从“人均 1 个”迈向“人均 5–10 个”，并发叠加效应下总带宽需求呈指数级攀升。园区网络的接入带宽正加速向 Wi-Fi 7 以及 2.5G/10G 接入演进。

趋势二：AI 应用推动企业业务平台间、数据流互联互通。AI Agent 将进一步加速企业数智化进程，原有独立垂直的应用体系和数据体系将开始向工作流和数据湖演进。园区网络需要构建融合架构，将有线、

Wi-Fi、蓝牙、楼宇物联网等各类异构网络融合，在承载数据传输的同时也兼具了融合感知的能力，为上层业务应用和 Agent 提供高质量的数据基础。融合建设模式能够有效降低总体拥有成本（TCO）并提升运营效率，例如结合接入、感知、定位等多维数据，经大模型推理分析后，通过 Agent 自动化执行，最终实现资产分钟级自动盘点、物料全流程追踪、车间绿色节能等一系列降本增效的运营举措。

趋势三：AI 应用加剧企业业务安全威胁。AI Agent 具备自主思考、任务规划与自主执行能力，随着其处理任务的增多，将为企业带来新的安全风险。园区安全开始从物理连接保护、终端资产接入保护、信息防窃听、空间防入侵等传统安全向智能体安全治理演进。网络安全的战略定位，正在彻底从“外挂式的防御”转型为新一代数字基建的底层核心资产与 AI 时代的核心生产力要素。传统园区网络所依赖的“边界筑墙、外挂安全”架构，在面对数字与物理空间双重交织的立体威胁时，由于缺乏对海量异构物联网资产的智能感知与自主决策能力，导致网络在边界告破、威胁横向无序扩散时陷入“资产失控、感知失明、阻断失能”的全面被动。面对这一安全鸿沟，网络与安全的深度融合以及 AI 原生赋能已成为不可逆转的时代趋势。下一代园区网络必须构筑“内生安全”新架构，进化为集“内网资产大模型毫秒级智控、无线全链路 AI 内生加密、物理空间全场景通感一体智能防御”于一体的安全防御体系，实现威胁的自动识别、秒级溯源与自主闭环。这不仅是技术层面的迭代，更是对数智化建网门槛的一次战略级拉高。

趋势四：AI 应用催生海量终端、智能体接入，终端管理和运维模式发生剧变。从以人为主的访问到以 Agent 自主访问的模式变化，执行任务从传统的单一应用访问到智能体同时访问多个系统工具，这些全新工作模式将会给园区网络的运维复杂度带来数十倍的提升。传统运维依赖人工排班与工单驱动，故障发现到修复常以小时计。而如今智能体开始 7×24 小时不间断执行任务，相应地要求网络运维必须要 7×24 小时的实时响应，在发生故障时能够快速自主实时感知，关联拓扑、自动识别异常并生成修复建议，经人机协同后能够自主进行处置，从而保障业务不间断运行。传统以人为主的运维模式与平台架构当前已无法满足 Agent 时代的业务诉求，网络必须要能够通过“自治”确保业务的持续运转。网络运维正从“人操作”迈向“人监督”——Agent 承担 7×24 小时监控、根因定位与自动修复，人类仅在策略决策点介入。当前主流网络厂商已经开始将 Agent 能力嵌入基础设施，园区网络正加速实现“自感知、自诊断、自愈合”的完全自治，网络管理员的角色也将从“救火队员”进化为“策略设计师”。

二、园区网络关键挑战

随着 AI 技术在园区业务的广泛使用，园区网络在接入带宽、融合承载、安全治理和运维管理四个维度上面临全新挑战。

挑战一：千兆接入带宽受限，以下行流量为主的传统流量模型将发生变化。由于人均终端将增加至 3~5 个，终端开始内置多 Agent 自主访问网络，多客户端、多 Agent 并行多模态交互导致上行流量占比增大。尤其是以上行并发流量为主的业务形态和传输模式，将对当前

针对下行流量进行统一调度的无线网络带来极大冲击。无线网络在应对连续组网下无线带宽将轻松突破 Gbps 的同时，还需解决多客户端上行竞争冲突的难题。园区接入交换机将加速向多速率演进，快速迈入万兆接入阶段，主干随之开始向 100Gbps/400Gbps 演进。

挑战二：传统烟囱式建网无法适应 AI 时代的园区业务模型。根据 Gartner 公开预测和麦肯锡机构报告，虽然已有 85%的企业完成或正在启动数智化建网，但多数仍停留在传统的“烟囱式”数据孤岛模式，导致各系统间的数据无法互通，完成一项任务需登录多个系统，企业整体运营效率受到极大影响。园区众多智能业务终端和物联终端使用各种物联协议标准，极度碎片化，导致传统企业园区并存多种连接方式（Wi-Fi/Zigbee/蓝牙/星闪/RS485/Modbus/LoRa）与物联协议（BACnet/Modbus）。融合建网要求“一张网”全承载，架构需兼容多种频段和协议。

挑战三：传统的网络安全技术在 AI 时代不再可靠。伴随大量行业终端和非标物联终端的接入，以及越来越多的流量被加密，传统的指纹库无法应对终端形态以及版本的快速更新迭代，30%以上的终端无法被识别，进而终端行为异常也难以被感知。网络底层看盲、管漏，无法做到精准的威胁研判。其次，随着 AI 技术和量子计算的兴起，传统加密算法的安全根基已被动摇，变得不再可靠。再次，网络遭受入侵时，流量往往已发生明显异常变化，但现有网络难以捕捉该异常并及时触发告警。最后，越来越多的终端开始内置 AI Agent，其自主行为更加难以辨别是否是正常行为，进一步加剧了园区的风险

管控难度。

挑战四：网络运维管理复杂度激增。未来五年，智能终端、哑终端、具身终端将以 Wi-Fi 为主接入网络。终端数量的增多、无线网络环境的动态变化、任务交互访问路径的多样化等因素，将导致园区网络运维管理的复杂性成指数级激增。传统以人工为主的运维方式已完全无法满足业务对网络作为“生产系统”所需的敏捷性和实时可靠性要求。

综上所述，为有效应对这些挑战，园区网络自身也需要借助 AI 技术来实现迭代更新，用 AI 对抗 AI 带来的挑战。一方面园区网络应不断提升自身的接入（尤其是无线接入）能力、融合承载能力和安全防护能力，以支撑和加速 AI 技术在企业场景中的落地发展；另一方面，也应积极利用 AI 技术解决一些传统网络管理中人工难以有效解决的问题，确保园区网络能够高速、安全地支撑企业业务。未来 5 年，园区网络将从单纯的“连接管道”向园区智能融合基座演进。万兆接入、无线融合、全域安全、网络自智将成为新一代园区网络的典型特征，是构筑下一代万兆 AI 园区网络竞争底座的战略核心。

三、万兆 AI 园区网络关键特征和技术

AI 业务的广泛应用，从**接入带宽、数据融合、安全治理**与**运维管理**四个维度对园区网络提出了全新挑战。为此，**万兆 AI 园区网络**围绕**万兆接入、无线融合、全域安全、网络自智四大特征**，构筑完整的技术体系。

首先，带宽是 AI 落地的第一道门槛。AI Agent 接管日常办公使

千兆带宽迅速耗尽，**万兆接入**以 Wi-Fi 7 和 10GE 有线接入提供端到端万兆能力，**彻底消除带宽瓶颈**。

其次，AI 应用不仅需要带宽，还需要来自物理世界的物联、环境感知与定位数据。**无线融合**将 AP 升级为统一的数据入口，为 AI 应用提供基础数据支撑，**打破数据割裂困局**。

再者，在 AI 具备感知和操控物理世界的能力后，安全威胁也随之从数字世界蔓延至物理世界。**全域安全**基于资产、连接、空间与隐私四个维度构筑纵深防护体系，**应对安全威胁的泛化**。

最后，AI 数量的增长使网络规模不断攀升，运维时效和运维复杂度已超出人力运维极限，必须引入 AI 能力进行治理。**网络自智**通过网络数字孪生与网络智能体实现网络的自主运行，**破解运维触顶难题**。

综上，万兆接入、无线融合、全域安全、网络自智成为 AI 时代园区网络的四大特征。**接入与融合构成连接与数据底座，安全全程护航，自智统管运行，共同形成万兆 AI 园区完整的技术体系。**万兆 AI 园区网络的整体架构如图 1 所示。

图 1 万兆 AI 园区网络架构图

（一）万兆接入

万兆接入从**有线、无线、确定性网络**三维度构建统一底座：**有线侧**向万兆演进以消除带宽瓶颈，**无线侧**以 Wi-Fi 7 进阶能力有效管理空口竞争，工业场景则引入 TSN 确保微秒级确定转发。

1.有线万兆演进

AI Agent 的规模化落地，使接万兆接入势在必行。然而，园区场景的现实条件千差万别:存量布线、新建空间、弱电间资源各不相同，AI 终端的部署密度与业务模式也各有侧重，带宽提升需基于实际约束，匹配**利旧、新建、极简改造**等不同场景。

面向利旧场景，大量的存量园区场景均部署了 Cat5E 或 Cat6 网线,全面重新布线成本高昂且施工困难。可以通过多速率以太网(mGE)技术，利旧线缆并将接入层带宽提升至 2.5Gbps。该方案无需更换线缆,仅需升级端口侧网络设备即可实现带宽翻倍,以最小的硬件成本,有效缓解 AI 终端并发带来的带宽拥塞。

面向新建园区或具备重新布线条件的改造场景，物理介质可以选 Cat6A 线缆或者光纤部署，全网采用统一的以太网及 IP 协议、提供独享 10Gbps 带宽接入能力，一步到位满足高性能终端速率要求。而针对光纤场景的供电需求,业界推出了新型光电混合缆提供光纤加供电的能力。

面向极简建网或弱电间受限等改造场景，如教育、医疗等房间密集型场景，无源以太网络方案采用“中心交换机—无源汇聚模块—远端模块”的极简架构。无源汇聚模块无需供电,可灵活安装于弱电间,

免去了传统汇聚层所需的独立机柜与供电设施，有效节省 75%的物理机柜空间。基于波分复用技术，无源汇聚模块在物理层完成光信号的分发与复用，使每个远端端口与中心交换机的逻辑端口一一映射，不存在传统以太网汇聚层的带宽收敛问题，上下行均可实现万兆独享。远端模块作为中心交换机的端口扩展，免配置即插即用，由中心交换机统一纳管，使管理网元数量降低 90%。针对不同建网场景的建网方案如图 2 所示。

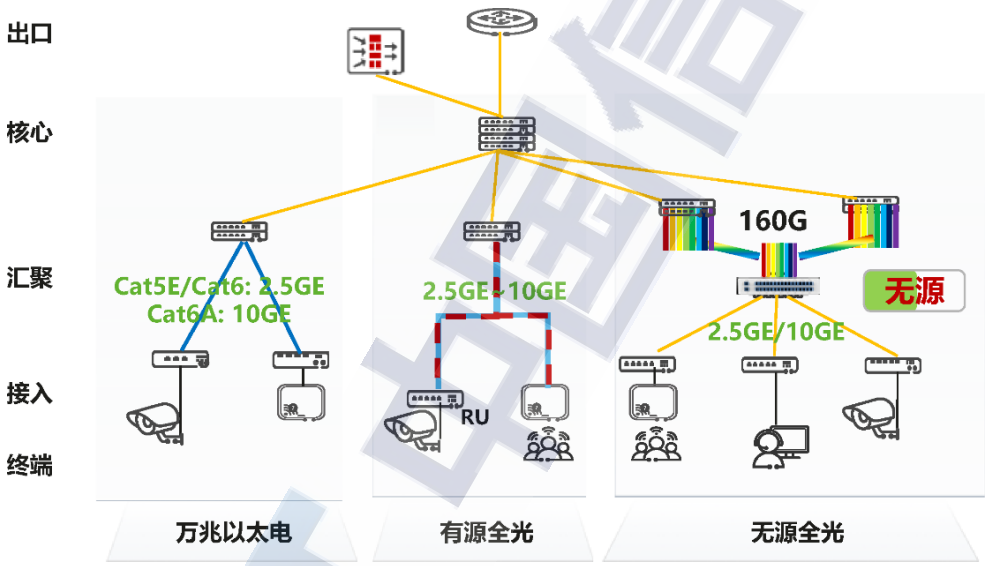

图 2 针对不同场景的建网方案示意图

2.无线接入跃升

无线侧的压力同样直接来自 AI 业务，高密区域密集 AI Agent 的并发运行、AI 数据和视频会议的资源争抢、具身智能终端的跨区移动，要求**无线网络**在**覆盖、空口带宽和并发、调度**和**漫游**四个层面进行针对性增强。

（1）**覆盖范围：**Wi-Fi 7 以 4096-QAM 高阶调制将理论峰值速率较 Wi-Fi 6 提升约 20%，然而高阶调制对信噪比的要求极为苛刻。AI

Agent 稍离 AP，信号衰减叠加射频功率放大器（PA）高功率输出时的非线性失真，接收信噪比便跌破高阶调制门限，4096-QAM 随即退化至 1024-QAM 等 Wi-Fi 6 时代的调制档位，理论峰值往往只能在 AP 下方约 1 米内兑现，其余位置仍是上一代速率。数字预失真（DPD）技术在发送侧对功放失真进行反向补偿，有效提升线性度与信号质量，将 4096-QAM 的可用范围从约 1 米扩展至 5 米，并增强信号强度，使高阶调制在实际场景下真正可用。数字预失真技术对覆盖范围的增强原理如图 3 所示。

图 3 数字预失真增强覆盖原理示意图

（2）**整网吞吐量和并发：**高密办公区域内，密集 AI Agent 终端并行工作，空口并发需求成倍增长。根据香农定理，无线网的吞吐量和频宽呈正相关，传统 20MHz 频宽组网已无法满足整网吞吐量的诉求，必须向 80MHz 频宽组网演进。然而，以中国 5GHz 频谱为例，80MHz 频宽下的可用信道仅有 3 个。可用信道数量的减少，意味着高密部署时同频 AP 之间的物理间距缩短，由此带来的同频干扰急剧增大，同频 AP 之间只能通过避让来避免冲突，导致整网实际吞吐量不升反降，频宽与带宽形成矛盾。解决该问题的关键在于将同频 AP

从“**互相避让**”变为“**协同调度**”：首先，相邻 AP 之间通过交互，实时测量各终端到多个 AP 的路径损耗信息，明确终端的位置分区；其次，根据分区结果，AP 的智能天线可自动切换工作模式，近端终端使用定向模式将信号能量集中，避免对其他 AP 的并发造成干扰，远端终端则使用全向模式，通过分时方式有序传输；最后，通过协同调度实现**近端并行同时发送、远端分时有序发送**，解决频宽与带宽的矛盾难题。多 AP 协同调度的技术原理如图 4 所示。

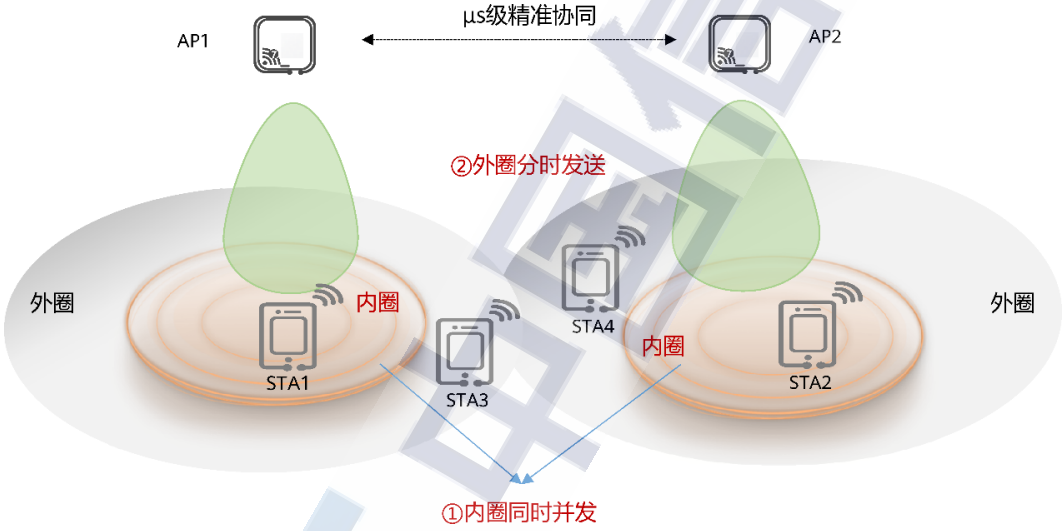

图 4 多 AP 协同调度原理示意图

（3）**精细化资源调度：同一 AI 终端往往同时产生两类截然不同的空口数据流：**一类是持续大吞吐的“**大象流**”（如模型训练数据上传、大文件同步），另一类是时延敏感的“**关键流**”（如实时视频会议、语音交互）。传统服务质量（QoS）限速手段会对所有流统一降速，导致关键流的音画同步受损。为解决此类冲突，需使用**精细化智能调度技术**，在**不依赖传统限速手段**的前提下实现关键业务的优先保障：首先可以对**空口资源进行预留**确保关键业务的绝对优先调度。其

次**使用精细化智能反压手段**，通过反压技术抑制上行贪婪流量。最后针对同频 AP 下的终端存在大象流互相影响的情况，通过**多 AP 协同的方式**，对同频 AP 下的大象流进行主动压制，保障所在信道内关键业务的优先调度。精细化资源调度的实现原理如图 5 所示。

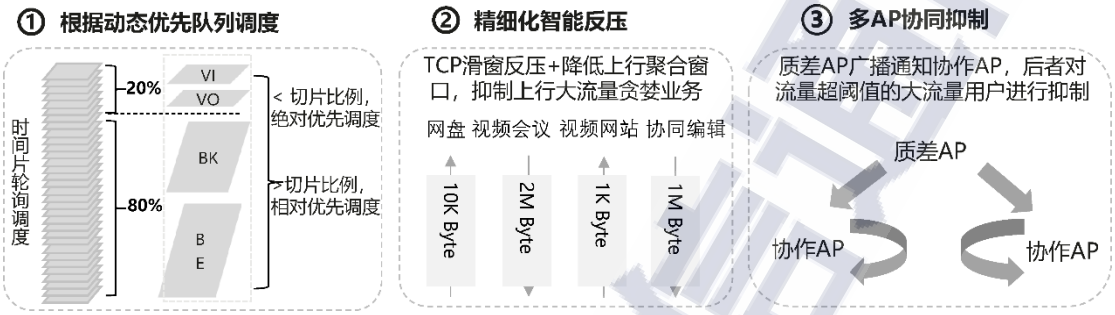

图 5 精细化资源调度原理示意图

（4）无损漫游：具身智能机器人已广泛应用于园区安防巡检及仓储物流场景。此类机器人同时具有高带宽的“感知数据流”与低时延的“控制流”，**跨区域移动时漫游切换引发的丢包将可能导致感知数据和控制指令丢失**，触发紧急制动或失联。特别是在多机器人协同作业中，单台中断可能引发连锁反应，影响整体节拍，因此**漫游零丢包**成为机器人稳定安全运行的关键诉求。

零漫游技术为解决上述问题提供了可行路径。其核心机制是将多台物理 AP 的基本服务集标识符（BSSID）统一合并为逻辑上的虚拟“大 AP”，并通过高精度时间同步实现 Beacon 帧的合并发送。在物理层多 AP 覆盖区域内，系统为每个终端动态选定一个最优服务 AP，其余同频 AP 作为监听节点。终端移动过程中，服务 AP 实时评估切换条件，一旦检测到更优候选 AP，即触发完全无感知的服务交接，无需重新关联认证，从终端视角看，漫游过程被完全屏蔽，实现了真

正的零丢包漫游。零漫游技术的原理如图 6 所示。

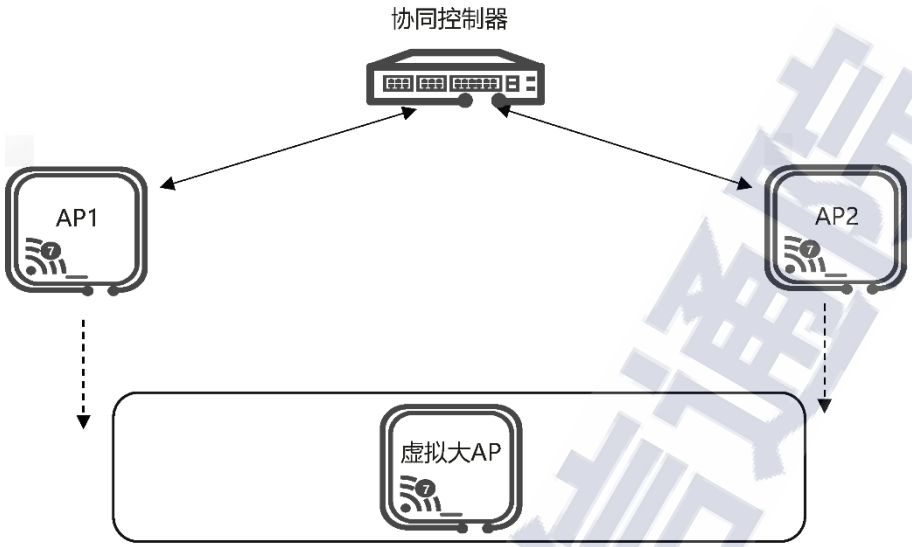

图 6 零漫游原理示意图

3.确定性低时延

在工业制造场景中，AI 机器视觉质检设备已规模部署于产线。此类设备需将 4K/8K 超高清图像实时回传至边缘 AI 服务器进行推理判断，同时产线上的可编程逻辑控制器（PLC）控制信号也需在微秒级内完成闭环。基于传统的尽力而为转发机制，一旦网络出现抖动或丢包，将导致推理超时、误检或产线紧急停机。

时间敏感网络（TSN）基于 IEEE 802.1Qbv 门控调度和 1588v2 高精度时钟同步，为控制信号等时延敏感型业务预留独立转发通道，提供微秒级确定性转发，使 AI 质检数据与控制指令按时、无损地抵达目标节点，保障产线持续稳定运转。TSN 确定性网络组网架构如图 7 所示。

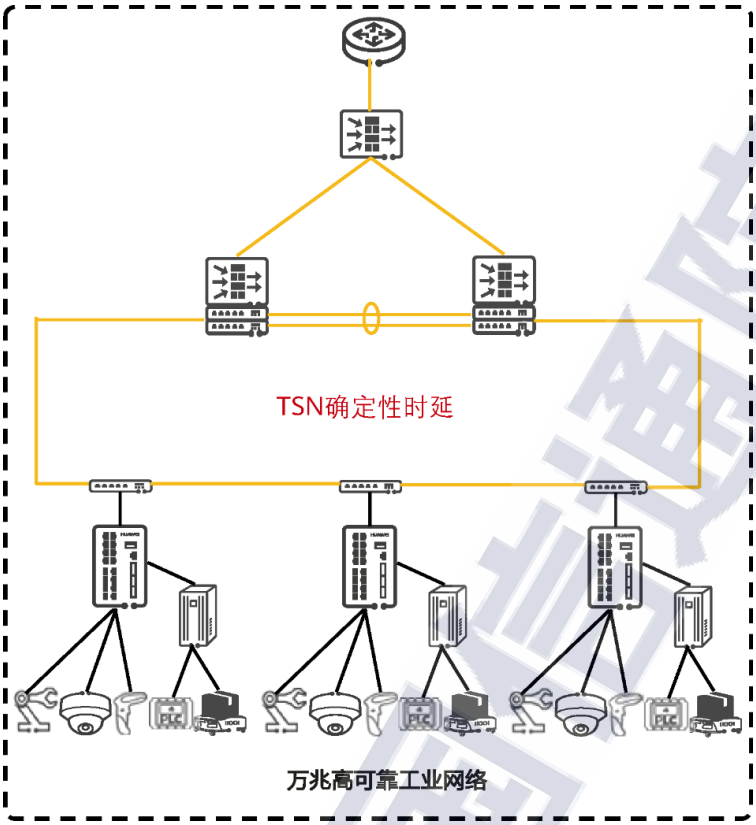

图 7 TSN 确定性网络组网示意图

4.关键指标

具备万兆接入特性的园区可提供如表 1 所示的网络能力。

表 1 万兆接入网络能力

分类	指标项	指标要求
万兆提速增质	无线：单 AP 160MHz 单用户极限速率	>=2Gbps
	无线：3 个 AP 80MHz 同频组网总吞吐	750Mbps
	无线：9 个 AP 80MHz 异频组网总吞吐	2250Mbps
	有线：接入侧上行带宽	支持独享 2.5Gbps
	长距增强型以太网供电（PoE++）能力（光电混合缆）	>=250(米)
	业务性能：1080P 高清视频路数/单 AP	50 路

针对存在更高业务需求的场景，可部署更高阶的万兆接入网络，其在无线带宽、网络并发性能等方面的能力如表 2 所示。

表 2 高阶万兆接入网络能力

分类	指标项	指标要求
万兆提速增质	无线：单 AP 160MHz 单用户极限速率	>=2.2Gbps
	无线：3 个 AP 80MHz 同频组网总吞吐	1140Mbps
	无线：9 个 AP 80MHz 异频组网总吞吐	3420Mbps
	业务性能：1080P 高清视频路数/单 AP	70 路
	有线：接入侧上行带宽	支持独享 10Gbps，支持切换 2.5Gbps
	有线：汇聚侧单端口带宽	支持单模块超 100Gbps，支持无源汇聚模块
	有线：核心侧单端口带宽	支持单模块 400Gbps
	可靠：支持无损升级	支持跨设备链路聚合组（M-LAG），50ms 业务切换
	可靠：环网场景高性能冗余保护	支持 10ms~20ms 故障切换
	可靠：工业高可靠零丢包冗余保护	支持高可用无缝冗余协议（HSR）/并行冗余协议（PRP）等无损切换协议

（二）无线融合

为打破传统烟囱式建网造成的数据孤岛与协议碎片化困局，无线融合将 AP 升级为“通感一体”锚点，原生融合物联、感知与定位能力，使网络从连接管道进化为智慧空间载体。无线融合“通感一体”的整体架构如图 8 所示。

图 8 无线融合“通感一体”总体架构图

1.物联融合

电子价签、资产标签、产线传感器、智能电表等物联终端，正是 AI Agent 感知现场、执行动作的数据来源。Wi-Fi 凭借其高并发、低时延特性，成为理想的统一物联接入平台，能够有效协同蓝牙、射频识别（RFID）等主流协议。通过在网络侧实现统一接入与管理，该方案显著简化了传统多协议物联网部署带来的架构复杂性与运维成本，为资产数智化提供高效、经济的路径。

- 高效支撑海量电子价签的实时信息同步与集中管控，赋能动态定价与库存可视。
- 融合 RFID 与蓝牙能力，轻松实现固定资产的自动盘点与移动物资的轨迹管理，提升资产利用效率。
- 为产线传感器、智能电表、环境监测终端等海量设备提供稳定可靠的无线接入，支持生产与能耗数据的实时回传。

2.感知融合

AI 应用需要感知物理空间的状态，例如空间安防需要及时发现非法闯入，楼宇节能需要判断房间内有无人员，健康看护需要感知

呼吸、跌倒等细微动作。Wi-Fi 信号本身成为感知媒介，结合毫米波雷达等专用传感，实现从“连接”到“认知”的跨越，实现真正的“通感一体”。

感知融合的技术基础是信道状态信息（CSI），空间内无人活动时，多径路径相对稳定，CSI 变化微小。一旦有人或物体移动，反射路径随之改变，CSI 的幅度与相位便出现特征性波动。AP 据此自发自收，即形成类似“声呐”的感知能力，无需任何额外硬件，可感知小至厘米级的运动：从人员存在、肢体动作，到呼吸引起的胸腔规则起伏，均可通过分析 CSI 的变化规律加以识别。AP 完成 CSI 数据的采集与计算后，可为上层 AI 应用提供空间感知数据。感知融合凭借免布线与多系统融合，显著降低部署与运维成本。

3.定位融合

随着 AI 业务深入园区物理空间，位置信息成为 AI Agent 决策的关键输入：商业运营需要客流热力分布以优化商业布局，巡检机器人需要定位以规划路径，安全管理系统需要追踪高危作业人员以触发即时预警。基于统一的 Wi-Fi 网络基础设施，可按需提供从区域统计到厘米级追踪的定位能力，精准赋能多样化业务场景，最大化基础设施投资回报。

- 接收信号强度指示（RSSI）定位（5-10 米精度）提供了一种极低成本的解决方案，非常适用于商超客流热力分析、楼宇人流量宏观统计等商业洞察与运营优化场景。
- 精细时间测量（FTM）定位（1-3 米精度）基于国际标准且智

能手机原生支持，能带来无缝的人员/资产定位、室内导航与电子围栏管理体验，提升访客服务与安全管理效率。

- 超宽带（UWB）融合定位（厘米级精度）通过 Wi-Fi 网络进行同步与回传，为高危作业人员安全监护（如定位安全灯）、贵重资产精确定位、自动导引运输车（AGV）与机器人导航等高要求场景提供可靠支撑。

4.关键指标

具备无线融合特性的园区可提供如表 3 所示的网络能力。

表 3 无线融合能力

分类	指标项	指标要求
无线融合	物联能力	Wi-Fi 7，星闪、蓝牙、Zigbee 等
	定位	UWB，FTM，RSSI
	物联网（IoT）扩展性	通用串行总线（USB），内置 IoT Radio，高速串行计算机扩展总线（PCIE）
	感知	WLAN CSI，毫米波雷达，非法摄像头
绿色节能	能耗潮汐预测	AI 预测
	快速唤醒时间	秒级
	整网设备能耗	降低 30%
	感知节能	支持 CSI 感知节能，Wi-Fi 感知有人/无人（含人员静止状态下的检测），联动空调、照明等开/关

（三）全域安全

当 AI 业务使终端类型日趋多样、接入行为动态多变时，传统

基于固定规则的安全防护难以有效应对。为此，**全域安全**引入 AI 能力对终端指纹、访问行为、流量模式等海量特征进行持续学习，识别未知终端，监测异常流量，安全防护从被动拦截向主动免疫演进。

这一主动免疫能力，根植于**全域安全**覆盖**资产、连接、空间、隐私**的四维防护体系，秉持“持续验证、永不信任”的零信任理念，以统一策略平台为中枢，整合多维安全能力，对用户、终端、数据、应用等全要素实施闭环管控，实现全对象、全流程、全空间的持续风险评估与最小权限控制。内生安全在威胁侵入的第一跳即完成发现、阻断与溯源，补齐东西向防护短板，将防护纵深从数据中心出口延伸到园区接入层，保障业务连续性与数据安全。在高安场景下，可使用专用密钥体系进一步增强端侧和无线空口的安全。全域安全的整体防护架构如图 9 所示。

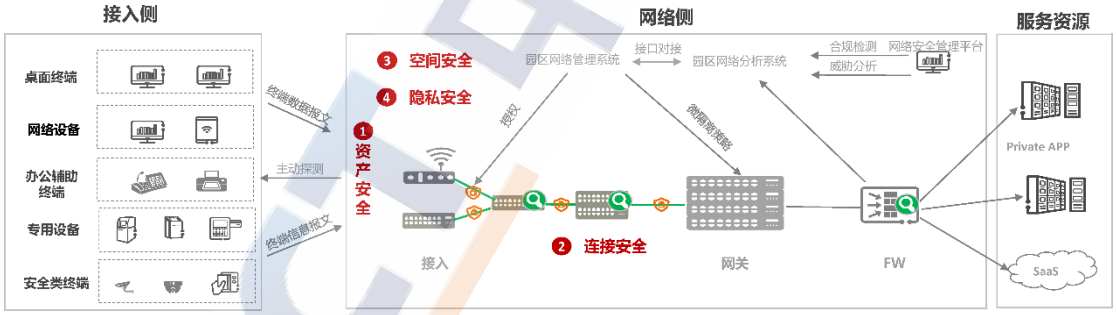

图 9 全域安全防护体系架构图

1.资产安全

AI 业务规模化落地使园区资产从传统的 PC、手机，扩展至 AI Agent、智能终端、物联网设备等海量新型实体，资产类型泛化、接入方式多样，传统基于设备指纹的静态识别手段难以覆盖，仿冒与挟持风险加剧。**资产安全**通过四道防线逐层递进解决资产安全问题。

第一道防线是资产识别。交换机内置探针通过被动指纹采集终端特征，结合主动扫描补充设备类型信息，对于广泛的行业终端以 AI 聚类算法进行流信息识别，实现对未知终端自动分类。这一能力从根本上解决了传统人工资产台账滞后于网络实际状态的问题。

第二道防线是准入认证。确保只有合法的终端和 AI Agent 能够接入网络，通过准入认证对用户和设备进行身份验证，控制企业内部和外部终端对网络的访问，实施统一的接入控制策略，同时提供灵活的认证策略和授权策略管理功能。

第三道防线是防私接与防仿冒。攻击者可能通过私接和仿冒两种方式绕开前两道的识别与认证: 私接指员工在工位私自接入无线路由器，在办公网内创建出不受管控的隐蔽子网，外部人员可通过该子网获得内网访问权限却不经过任何准入检查; 仿冒指攻击者将自身设备的媒体访问控制（MAC）地址等标识修改为已授权终端的对应值，在身份层面伪装成合法资产。针对私接，可通过检测交换机端口下的生存时间（TTL）跳数异常、动态主机配置协议（DHCP）指纹等特征进行识别；针对仿冒，可通过比对终端操作系统协议栈指纹、浏览器版本组合等多维度行为特征与资产基线库的差异进行判别，解决恶意终端仿冒渗透进入内网的问题。

第四道防线是 AI 异常流量分析。前三道防线覆盖了从识别到认证再到私接仿冒的完整链路，但仍存在一种场景令其失效。例如，一台已通过准入认证且多维度指纹均正常的摄像头，其固件因漏洞被远程利用并植入恶意代码。此时，该摄像头在资产识别、准入认证、防

仿冒三个层面均表现为正常设备，但与外部攻击者正在隐蔽通信、对内网其他主机的扫描行为已构成实际威胁。对于这类合法终端被控的场景，通过在接入交换机中持续学习每类终端的正常通信基线，捕捉偏离基线的异常模式，例如摄像头的违规外联或通过摄像头进行内部文件窃取导致流量异变，交换机可以在秒级识别并自动执行端口隔离作为最后一道防线，从网络层切断攻击路径，同时将事件上报管理平台供安全团队研判。

2.连接安全

AI Agent 的每一次工具调用与数据回传，其流量都需依次穿越空口与有线两段链路。这意味着整条路径的防护强度取决于其中最薄弱的一环，攻击者的突破口往往就选在空口的开放信号或有线链路的物理暴露点上。在空口侧，无线侧利用 Wi-Fi 信号的开放传播特点，通过空口窃听截获数据包；在有线侧，AP 上行链路和交换机之间链路处于开放环境，可以通过窃听等手段直接截取明文流量。如果仅加密其中一段而另一段明文传输，则整条链路的防护即告失效。

在空口侧，通过物理层加扰进行保护。无线局域网（WLAN）的数据安全主要依赖对称/非对称密码学加密方案，如 Wi-Fi 保护访问第二版（WPA2）、Wi-Fi 保护访问第三版（WPA3） 协议中的高级加密标准（AES）加密算法等，这些技术通过加密数据来保护信息传输的安全性。在 WPA2 时代，出现过密钥重装攻击（KRACK）等基于安全协议漏洞的安全事件，**物理层加扰技术**正是针对这一弱点，不依赖任何上层密钥，通过信道探测获取合法用户的精确位置信息，再利

用波束成形在合法用户位置以外的空间区域发送定向随机噪声信号，窃听方即使处于 AP 信号覆盖范围内也只能捕获无意义的噪声而无法解调出有效数据帧，而正常用户通信不受影响。WPA3 叠加**物理层空口加扰技术**，相当于给链路传输加了“双重保险”，使得无线信号即使被截获也无法破解，彻底解决了企业对无线办公的安全顾虑。物理层空口加扰的原理如图 10 所示。

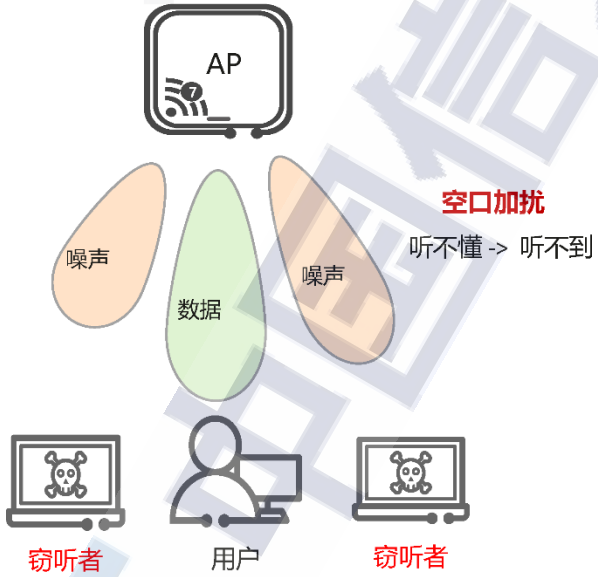

图 10 物理层空口加扰原理示意图

在有线侧，通过媒体访问控制安全（MACsec）逐跳加密进行保护。因为 AP 到交换机的上行链路，以及跨楼栋的交换机之间的光纤处在开放环境，存在被窃听风险。MACsec 基于 IEEE 802.1AE 标准在数据链路层实现逐跳加密与完整性校验，从 AP 上行到交换机的有线链路即开始加密，后续经汇聚交换机、核心交换机，每一段链路上的数据帧均由硬件芯片完成加密和校验，对数据转发性能无影响。同时 MACsec 支持 SM4 国密算法。MACsec 端到端链路加密的路径如

图 11 所示。

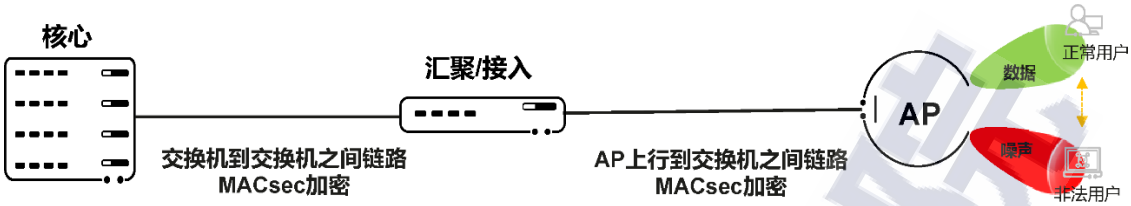

图 11 MACsec 端到端加密路径示意图

在密码体系演进层面，通过抗量子密码（PQC）进行保护。面向未来，量子计算的发展对传统 RSA、椭圆曲线加密算法（ECC）等非对称加密体系构成了实质性威胁。PQC 基于可抵御量子攻击的数学难题构造，通过算法升级即可部署于现有网络，覆盖身份认证、密钥协商、数字签名等关键安全环节，PQC 可跟随算法演进而持续更新，实现抗量子破解能力的平滑增强。园区网络对 PQC 方案的落地，从管理面、控制面、数据面等多个维度考虑抗量子改造。管理面与控制面通过扩展 PQC 密码套件，将密钥协商算法替换为基于模格密钥封装机制（ML-KEM）；数据面同样在密钥协商阶段引入 ML-KEM，采用 AES-256 对称加密，根据业界对 Grover 算法的评估，AES-256 等效强度约 128 比特，具备充足安全余量，从而保障管理、控制及数据通道的传输安全。

3.入侵监测

园区中存在大量摄像头难以覆盖或不宜部署的敏感物理空间，包括高密会议室、高管办公室、档案室等。这些区域一旦发生非法入侵，传统安防手段无法及时感知。空间安全利用 AP 内生的能力，在不增加额外传感器的条件下，基于 CSI 信息利用 AI 算法实现对这些安防

盲区的全天候监测。

CSI 人员存在感知技术通过分析无线信号在空间传播中的信道状态变化，感知人员的进入、离开。该技术仅分析信号扰动的物理特征，不涉及图像采集或个人身份识别，在实现空间安全的同时保障个人隐私。单台 AP 覆盖约 10 米范围，检测到非授权人员进入时秒级生成告警并联动安防平台。人员感知原理如图 12 所示。

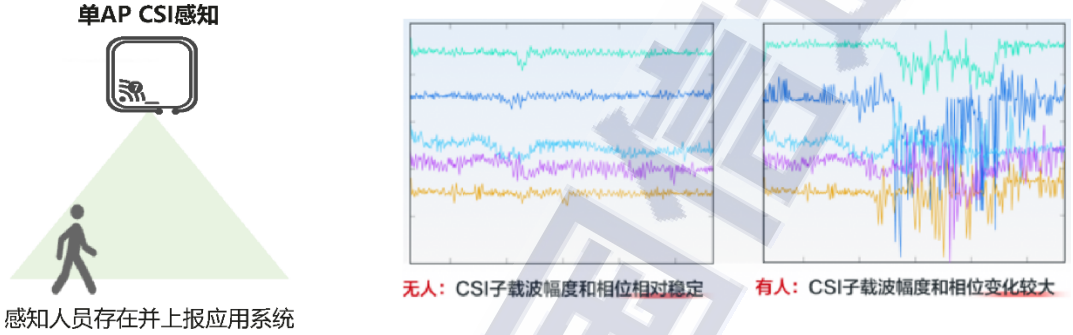

图 12 人员感知原理示意图

4.偷拍防护

在酒店客房、机密会议室、高管办公室等高隐私场景中，针孔偷拍已成为核心安全隐患。传统人工排查、红外扫描、射频探测等手段效率低、漏检率高、难以实时防护，且易受环境干扰；加之非法摄像头日趋微型化、隐蔽化，支持本地存储及 4G/5G 回传，不依赖 Wi-Fi 即可工作，进一步加大检测难度，使个人隐私、商业机密与政务信息面临严重泄露风险。

针对这一挑战，可利用 AP 感知电子设备的电磁特征信号，利用 AI 算法对感知到的电磁特征进行实时分类，实现对 Wi-Fi、蜂窝网络及本地存储类针孔摄像头的有效检测。该技术能主动扫描周边空间、辅助人工精准排查。依托园区网络中的 AP 进行 7×24 小时自动监测，

持续识别疑似摄像设备并评估风险，显著降低人工排查成本，从而提供主动、全域、全天候的隐私防护能力，全面保障用户隐私与信息安全。隐蔽偷拍设备主动检测方案原理如图 13 所示。

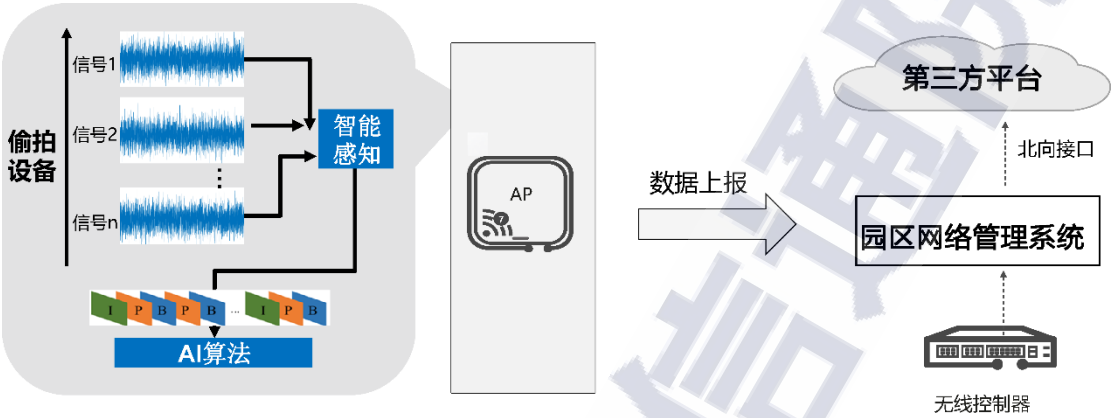

图 13 隐蔽偷拍设备检测原理示意图

5.关键指标

具备全域安全特性的园区可提供如表 4 所示的网络安全能力。

表 4 全域安全能力

分类	指标项	指标要求
终端内生安全	支持终端信息识别	支持被动流量分析、主动扫描识别资产。支持 AI 聚类实现终端识别
	威胁阻断	支持终端威胁场景联动交换机阻断网络访问
	基于零信任理念实现终端的安全合规准入	支持 30ms 快速私接检测（交换机内置），支持端点检测和响应（EDR）安全 Posture 检测
	准入终端基于业务实现安全隔离，避免风险横向扩散	支持 VxLAN 隧道方式和兼容三方独立部署方式
连接安全	无线安全加密	支持 WPA3、无线局域网鉴别与保密基础结构（WAPI）

分类	指标项	指标要求
	空口防窃听	支持空口加扰防窃听
	有线安全加密	无线上行和有线全链路支持 MACsec 安全加密，有线部分支持 AES256 和 SM4 算法

针对存在更高业务需求的场景，可部署更高阶的全域安全能力，其在终端内生安全、连接安全、空间和隐私安全等方面的能力如表 5 所示。

表 5 高阶全域安全能力

分类	指标项	指标要求
终端内生安全	终端安全合规准入	支持终端接入认证，支持内置 30ms 快速私接检测，支持终端安全检测和网络联动
连接安全	支持量子安全	通过 PQC 等机制支持抗量子安全，保障链路安全
	支持业务安全隔离	支持端到端 SLA 质量保障（如切片），支持软件定义网络（SDN）一键式部署
空间和隐私安全	空间感知安全	通过 CSI、毫米波等技术实现人员入侵检测和人身安全探测（如跌倒）
	非法摄像头检测	依靠网络支持非法摄像头探测

（四）网络自智

AI Agent 以 7×24 小时不间断执行业务，使网络保障不再有间歇，人工运维在时效与覆盖上触顶，网络运维必须利用 AI 进行治理。网络自智包括网络数字孪生与网络智能体。网络数字孪生是数据底座，

基于 SDN 技术提供园区数据采集和标准化加工，实现物理网络的精准数字映射。**网络智能体负责决策与执行**，通过网络设备提供基于 AI 的边缘决策能力，推动园区向自感知、自决策、自愈跃升。网络自智应用架构如图 14 所示。

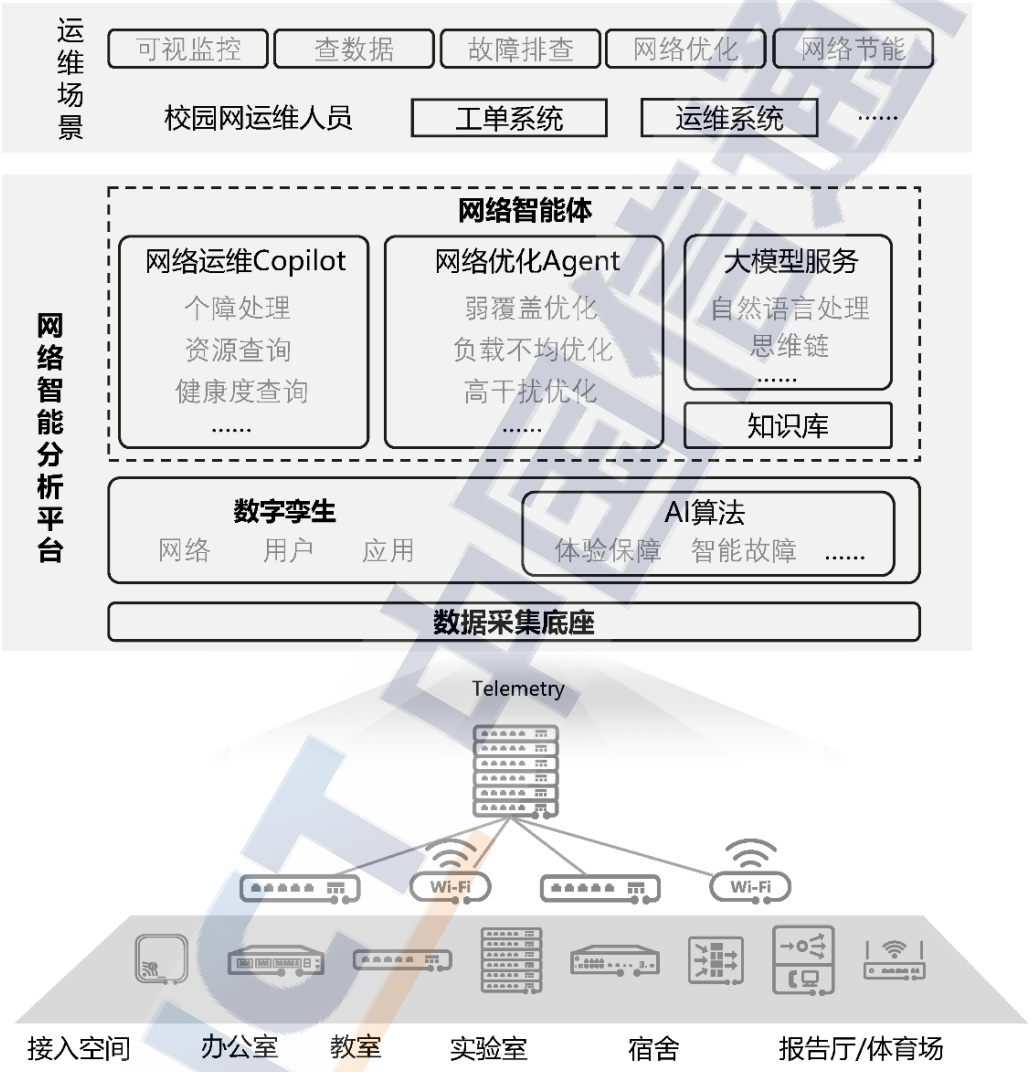

图 14 网络自智应用架构

1.网络数字孪生

网络数字孪生是在数字空间中构建与物理网络实时同步、精准映射并能进行深度交互的“虚拟镜像”。核心目标是实现“规划即所见、建设即所得、运维即所优”。依托交换机、无线控制器（AC）和 AP

的高精度遥测(Telemetry)技术，数字孪生还原流量拓扑与终端轨迹。通过随流检测（ In-situ Flow Information Telemetry ）深度关联网络、设备、应用三层指标，实现秒级故障定界定位。整网多维数字地图以时空图的形态呈现从全局拓扑到单个用户应用体验的全维度信息，支持七天内任意时间点的应用级旅程回放。基于时序深度学习算法，数字孪生可针对接口流量、光模块性能、AP 信号等指标进行长时间训练，预判健康变化趋势并推演能力临界点，提前发出规格超限或业务失效预警，将运维从“事后响应”转向“事前预警”。

2.网络智能体

数字孪生为网络建立了实时感知能力，而网络智能体则在此基础上承担决策与执行的角色。网络智能体由两个核心组件构成：一是面向网络自主运行的优化 Agent，执行自动化的故障处置与调优操作；二是面向运维人员交互的网络运维 Copilot，提供自然语言驱动的诊断与建议能力。

优化 Agent 以 7x24 小时自动运行的形态守护网络健康。它持续感知 AP 部署位置、环境干扰和终端网络体验状态，一旦发现弱覆盖、高干扰等典型无线问题，即在覆盖、干扰、频宽、负载等多个维度中统筹求解最优处置方案并自动执行。这一过程类似解一道 N 元 N 次方程：传统人工调优每次仅能考虑单一变量，而 Agent 在多个相互影响的变量之间寻找全局最优解，执行后自动验证效果并迭代优化。

网络运维 Copilot 改变了传统的命令行交互模式。运维人员以日

常语言描述问题，例如该用户下载慢请定位原因，系统即可理解意图，自动调用数字孪生中该用户的漫游旅程、网络体验质量、设备状态等数据，在网络数字地图上高亮问题节点，并推荐针对性的优化方案。这种以自然语言输入、以数字地图呈现的交互方式，将运维门槛从需要掌握协议细节和命令行操作降低到能描述问题即可，使过去依赖专家经验的故障诊断能力转化为系统化的组织能力。

综合 Agent 的自主执行和 Copilot 的交互能力，网络智能体可将典型故障实现从发现到修复的全流程自动闭环，减少用户投诉，缩短问题定位时间，保障关键业务的稳定运营。

3.关键指标

具备网络自智特性的园区可提供如表 6 所示的能力。

表 6 网络自智能力

分类	指标项	指标要求
网络自智	无线智能网规	计算机辅助设计（CAD）图纸、3D 仿真，支持 AI 识别绘制障碍物和 AP 自动布放
	设备即插即用	支持零配置部署（ZTP）
	支持多层数字孪生可视	精准感知网络状态，支持网络、用户、终端、应用多层数据可视

针对存在更高业务需求的场景，可部署更高阶的网络自智园区，可提供如表 7 所示的能力。

表 7 高阶网络自智能力

分类	指标项	指标要求
网络自智	设备即插即用	支持安全零配置部署（SZTP）
	无线网络故障自处置	支持无线故障自检测，接入类/体验类报障 85%自闭环，问题分钟级定界定位
	AI 大模型智能运维	大模型自然语言交互，支持状态巡检，Agent 智能问题闭环等

四、万兆 AI 园区网络典型应用

（一）万兆 AI 赋能智慧校园

1.趋势与要求

全球教育体系正加速向智能化转型，智慧教室、AI 个性化学习、AR/VR 沉浸式课堂及在线教学等模式，依赖高带宽、低延迟的校园网络，以保障教学效果与资源共享。科研场景中，AI 辅助实验预测与海量数据分析涉及 GB 级乃至 TB 级数据的实时交互，要求网络具备超高带宽和极低延迟。面对数万师生及多业务场景，传统人工运维效率低、故障处理慢，亟需建设全局可视的智能运维平台，实现快速感知与自动闭环处置。

上述趋势对校园网络提出了 2 个核心诉求：以万兆带宽底座支撑高带宽教学与科研场景，以 AI 大模型重塑运维范式。

2.典型应用

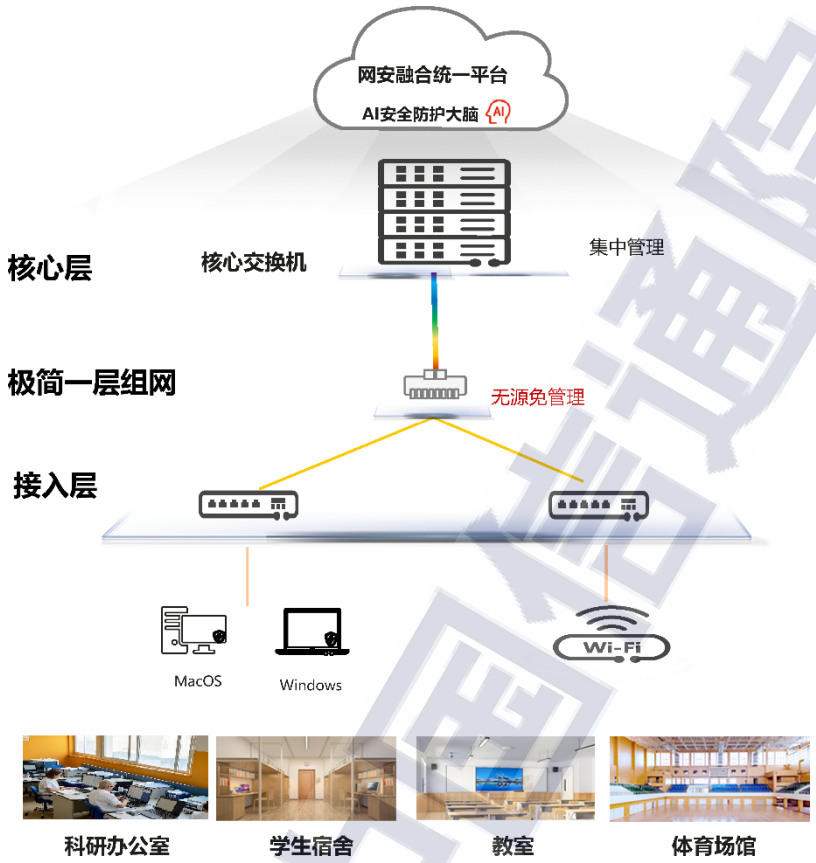

图 15 智慧校园网络架构图

（1）高速教学

《教育强国建设规划纲要（2024—2035 年）》明确提出“推进智慧校园建设”，在政策驱动下，VR 虚拟仿真教学、4K/8K 高清互动课堂等新型教学模式加速落地。然而，传统校园网络以千兆架构为主，接入层端口带宽仅 100Mbps，难以适配高清直播、在线教学、多终端并发等大带宽需求，高峰时段视频卡顿率超过 30%、时延 200ms 以上，网络基础设施的升级换代已成为高校高质量发展的迫切课题。

如图 15 所示，智慧校园网络超宽底座由无线超宽和有线超宽构成，通过无源以太网络方案，骨干带宽达 160Gbps 且全程不收敛，用

户侧实现万兆(10Gbps)入室，桌面终端可享 2.5Gbps/10Gbps 弹性接入。一间教室可同时支撑数十路 AR/VR 或 4K/8K 视频，科研团队秒级下载 GB 级数据，多终端并发无瓶颈。在报告厅等学生高密聚集的场景中，同频 AP 间的信号干扰往往是网速变慢的主要因素之一，可以通过 AP 间微秒级（us 级）协同帧调度，大幅降低 AP 间同频干扰，数百名学生同时观看高清视频、在线互动或提交大文件时，依然流畅不掉线，让校园网真正迈入“万兆接入”时代。

案例：随着智慧教学加速推进，某大学开始引入视频教学、AI 个性化学习、VR 课堂等智慧化教学方式，单教室带宽需 1Gbps 以上，但现有网络带宽一个教室仅有百兆，无法支撑 80 人教室 4K 教学，网课高峰期网络卡顿，并发干扰严重，且现网设备老旧，网络扩展性差，改造难度高。部署无源以太网络方案和动态校准技术后，10Gbps 光纤直达教室，免弱电间设计，简化网络架构，支持百人 4K 在线课堂，支撑最大可超 30 路高清 VR 视频同步传输，改造后在线教学卡顿投诉率下降超 90%，学生网课满意度评分由 3.8 分提升至 4.9，良好的教学效果有力保障智慧教学数智化转型。

（2）智能运维

随着智慧校园建设的深入，在线教学、科研协同及综合管理等核心业务快速发展，高校网络承载的业务规模持续攀升。面对万级网络设备、十万级终端接入及多厂商异构管理的复杂环境，传统依赖人工巡检和经验排障的运维模式已难以满足高效保障需求，运维体系正加速向智能化演进，AI 大模型驱动的智能运维成为行业新方向。清华

大学、上海交通大学等高校已率先引入基于 DeepSeek 大模型的智能运维平台，实现自然语言交互排障——运维人员只需说“东区宿舍卡顿”，系统自动调取关联设备日志、定位根因并推荐修复方案，构建“大数据 + 大模型 = 大运维”体系，实现自然语言交互与故障自主处置。

在校园网络运维中，网络故障与体验劣化等问题严重影响实时类业务。引入 AI 流量分析技术，可实现全路径可视，分钟级定位卡顿、掉线等网络质差问题，快速定位性能瓶颈。结合 AI 全局决策引擎，可自动完成整网优化与空口拥塞调优，实现 80%的无线故障分钟级的问题定位与恢复，显著提升校园网络运维效率与业务保障能力。

案例：某大学拥有 7 万+师生，3 万+网络设备和 17 万+终端，但网络运维老师仅 3 位。面对远程教学、在线课堂教学等高频业务，每月报障 200 多次，依赖经验排障的处置方式效率不足，工单处理平均时长大于 2 天。依托 AI 技术实现 80%的无线网络故障自动闭环，自动实时的网络体验优化让报障数量下降超过 80%，工单闭环时间缩短至 2 小时，师生满意度显著提升。

（二）万兆 AI 赋能电子政务

1.趋势与要求

《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14 号）明确提出推进一体化协同办公体系建设，持续增强电子政务外网移动接入能力与服务功能。同时，需要强化安全底座，加快关键核心技术攻关，全面加强关键信息基础设施安全保障，推动安全防护技术

深度应用，构建全方位、多层级、一体化的网络安全防护体系。以此为基础，文件确立了到 2035 年建成整体协同、敏捷高效、智能精准、开放透明、公平普惠的数字政府远景目标。网络方案在设计之初即对标等保 2.0 三级要求及商用密码应用安全性评估标准，确保安全能力与合规要求同步建设。

基于上述指导意见，需提供高安全电子政务网络解决方案，如图 16 所示。该方案在接入侧强化终端精准识别与管控，在传输侧聚焦数据加密与通道安全，筑牢端到端安全防线。

2.典型应用

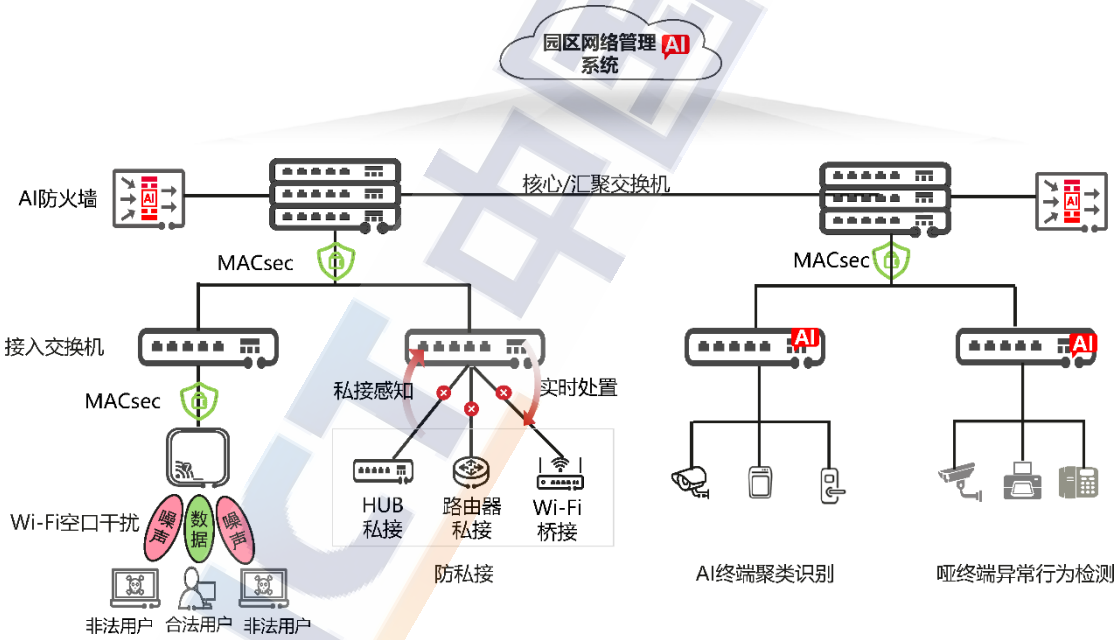

图 16 电子政务网络架构图

（1）电子政务资产安全

随着电子政务终端数量激增、终端类型日趋复杂多样，精准盘点终端资产已成为网络安全管控的首要前提。然而，人工管理不仅效率低下，更无法感知私接、桥接等隐蔽违规行为；同时哑终端因不具备

安全代理能力，即使被恶意劫持或仿冒，其异常流量也极易淹没在海量正常通信中，传统手段几乎无法察觉。这些“不可见、不可管”的资产盲区，为仿冒终端入侵政务外网、数据外传等攻击行为埋下严重隐患。

依托网络设备指纹识别、主动扫描和与终端 AI 聚类技术，电子政务网络实现全量资产可视，建立动态更新的资产图谱。在可视基础上，网络可主动探测私接路由器、Hub 及 Wi-Fi 桥接等违规行为，一旦发现即自动执行近源隔离。同时，针对被劫持哑终端，通过 AI 对其流量及行为进行持续实时检测，一旦发现静默设备突发外联、非业务时段活跃、流量特征偏离基线等异常，立即告警并联动近端阻断。支持接入位置回溯与用户身份关联，确保异常终端可识别、可阻断，并满足等保 2.0 及密评合规审计要求，实现安全事件全生命周期可追溯。由此，构建起覆盖“识别—准入—阻断—溯源”全流程的安全防线，为数字政府建设筑牢网络根基。

案例：某区政府办公园区长期依赖手工录入终端资产，耗时费力，且难以满足应急响应时效。按重保及上级要求，发生安全事件或接报问题 IP，须 30 分钟内定位责任人，超时将面临持续通报。为此，该区依托终端 AI 聚类技术进行资产识别，自动识别率达 91%，辅以少量手工标记，即可实现园区终端 100%可视化管理。终端安全事件 10 分钟定位到责任人，避免在重保活动中持续通报问题不解决，提升电子政务网络安全防护水平。

（2）电子政务连接安全

政务外网承载大量敏感隐私数据，涵盖个人身份信息、生物特征及企业商业数据等，一旦发生数据泄露，将造成严重的社会影响和法律责任。然而，政务园区 Wi-Fi 的普及拓宽了网络边界，使无线空口窃听与有线链路中间人攻击的风险显著加大。

为解决上述风险，无线侧在终端认证和数据加密基础上，进一步对空口物理层数据进行保护，通过 AP AI 空口加扰技术，在合法终端 6cm 范围外将干扰信号与有效信号叠加形成无法解调的信号，使得窃听者仅能接收到杂乱数据，而合法用户不受任何影响，从源头杜绝空口数据被侦听的可能。在有线侧，从 AP 上行到核心交换机全线支持 MACsec 链路层加密，实现有线链路防窃听、防篡改。空口加扰与有线加密双重防护，构建端到端全链路安全传输体系，从技术层面筑牢政务数据零泄漏防线。

案例：某区面积 132.39 平方公里，常住人口 63 万，其政务外网承载 63 万人的敏感隐私数据，涵盖个人身份信息、生物特征、社保账户及 3.2 万家企业商业数据等。为有效防范无线环境数据泄露风险，该区采用 Wi-Fi AI 空口加扰技术，叠加 AP 上行链路至核心设备部署 MACsec 链路层加密，构建端到端全链路安全传输体系。经实测，AI 空口加扰技术使窃听者捕获的有效数据还原率趋近于 0，可有效防御无线空口窃听与中间人攻击，确保隐私数据的机密性与完整性，从技术层面筑牢用户隐私零泄漏防线。

（三）万兆 AI 赋能安全金融

1.趋势与要求

随着 2025 年《中国人民银行业务领域数据安全管理办法》正式生效，金融行业安全监管迈入全面升级阶段。该办法明确要求数据处理者健全终端设备安全管控策略，并加强相关终端设备的准入控制。在此背景下，园区网络已不再是单纯的连接通道，而是承载合规要求与业务连续性的关键防线。

基于人行上述要求，需构建高安全金融园区网络解决方案，其典型架构如图 17 所示。该方案同时具备以下核心能力：以大带宽、低时延保障安全合规业务的高效承载；以 AI 驱动终端全量识别与准入控制，杜绝非法接入。

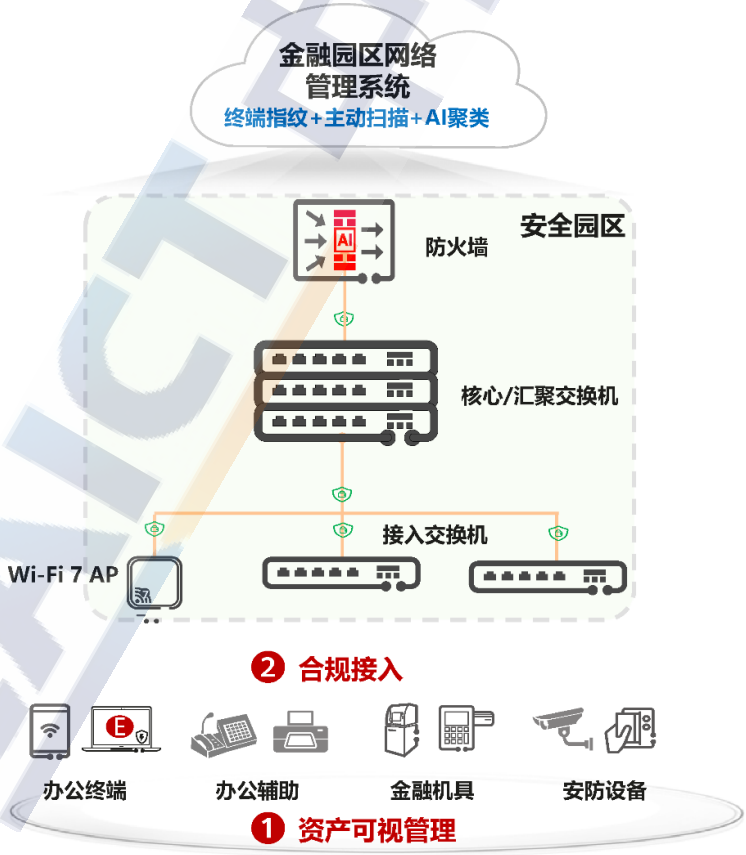

图 17 金融安全园区网络架构图

2.典型应用

（1）金融万兆接入

当前，金融数智化转型正以“十五五”规划为顶层牵引，围绕 AI 合规应用与数据价值深度挖掘，驱动行业从规模扩张向质量跃升转变。2025 年底发布的《银行业保险业数字金融高质量发展实施方案》进一步明确，IT 基础设施规划需前瞻布局 AI 大模型训练、推理以及海量数据实时处理所需的网络容量——预计每用户带宽需求将从当前的 4Mbps 增长至 50Mbps 以上，单 AP 并发连接数需支持 200+终端同时活跃。

与此同时，金融 AI Agent 架构已从传统的单 Agent 独立完成任务，演进为自主拆分任务、多 Agent 协同并发执行的新模式，整体处理效率显著提升，但这对底层网络的无线和有线网络并发承载能力也提出了更高要求。为应对这一挑战，无线部分通过多 AP 协同连续组网的方案，可大幅提升网络并发性能，有线部分采用 mGE 交换机拓展接入带宽，可有效支撑金融 AI Agent 的辅助处理过程，充分满足金融行业高并发、低时延的数据处理需求。

案例：某金融公司新建办公大楼，采用 Wi-Fi 7 + mGE 万兆园区方案。有线部分，接入速率最高支持 10Gbps；无线部分，采用多 AP 协同组网技术，在 30 用户 60+终端高密并发场景下实测，网络吞吐量提升 3 倍，单用户带宽从 4Mbps 提升到 12Mbps，确保会议室等高密场景下 AI 辅助金融数据处理分析依然流畅运行。超大带宽保障运营和风险管理部使用 AI 辅助金融数据处理分析流畅运行，夯实网络服务根基，全面提高金融业务响应速度。

（2）金融终端管理

2022 年，银保监会发布《关于银行业保险业数字化转型的指导意见》，正式拉开金融行业系统性推进数字化转型的序幕。经过四年多的发展，银行保险业业务效率与客户体验均得到显著提升。然而，随着转型深入，办公网与业务网中的终端种类和数量急剧膨胀，从传统 PC 到各类智能柜员机、移动展业设备、物联网传感器等，管理难度大幅上升，已成为保障金融网络安全与运营稳定的关键环节。

当前，终端管理面临两大核心挑战：一是大量新型及非标金融终端缺乏对应指纹库，传统基于特征库的识别方式难以有效覆盖；二是部分终端采用加密传输协议，导致常规指纹匹配规则失效，进一步削弱了资产可视性。针对上述难题，采用被动指纹采集、主动扫描探测与 AI 聚类分析相结合的技术方案。通过 AI 聚类技术解决传统手段难以识别金融专用机具的问题，提升资产识别率，构建立体化、智能化的终端识别能力。该方案能够实现对金融园区网全量资产的可视、可管、可控，从根本上杜绝非法接入风险，确保网络准入安全可靠，为数字金融业务的持续创新筑牢坚实底座。

案例：中国某银行，拥有数千种类型、数百万台的 IT 终端，由于终端种类庞杂、识别率不足，长期无法全量可视化管理，存在重大安全隐患。银行通过在国内一级行旁挂探针，海外分支采用嵌入式探针的部署方法，采集终端数据上报控制器，通过 AI 聚类资产识别方案，实现终端 100%感知接入，金融机具及办公哑终端资产

识别率 95%以上，结合自定义标注，最终达到资产 100%识别，增强金融终端的准入控制，完善金融资产的安全管控策略。

（四）万兆 AI 赋能智慧医院

1.趋势与要求

随着 AI 技术高速发展，医疗智慧化持续迭代，推动“医疗+AI”模式在提升诊疗效率、促进医疗普惠、推动优质资源下沉等方面释放效能。依托智慧医院建设，实现院内数据互联互通，并配以完善的数据安全与智能预警系统，提升运行效率，为群众提供更优质的服务。

国家统计局数据，2025 年全国门急诊总医疗人次为 105.8 亿，出院人次为 3.0 亿。面对巨大的诊疗需求，优化诊断数据流转效率、提升医护工作效率，已成为推进医院智慧化转型、提升服务质量的关键举措。

2.典型应用

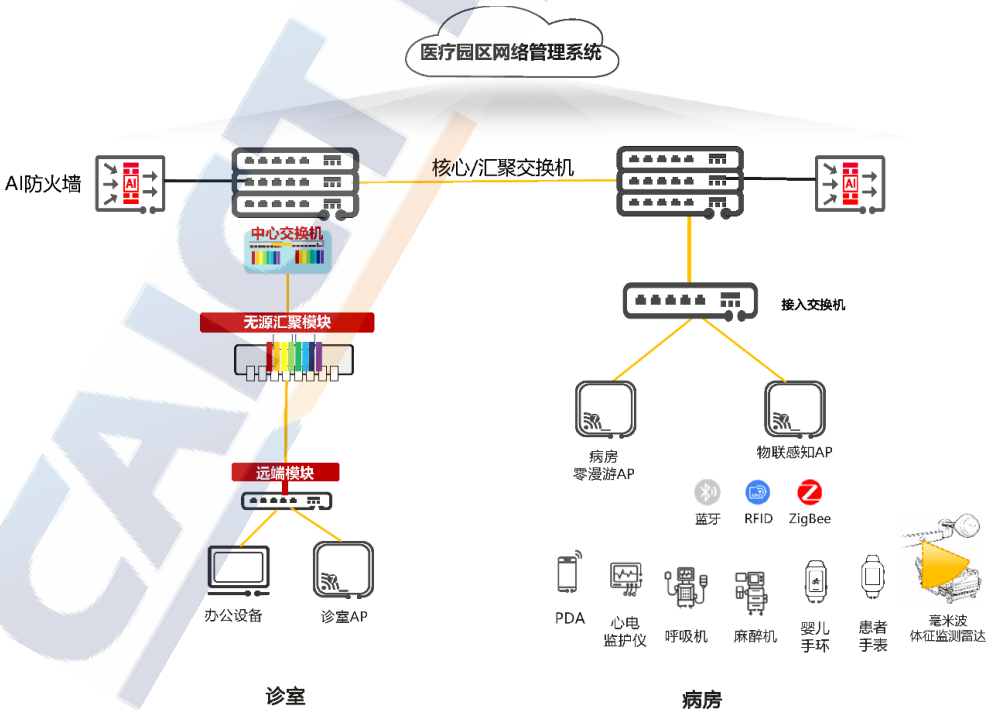

图 18 智慧医院网络架构图

（1）高速品质医疗网络

在日常查房工作中，医护人员持个人数字助理（PDA）穿梭于病房之间时，传统 Wi-Fi 漫游丢包严重，频繁掉线、重连导致医嘱和生命体征数据无法实时上传，诊疗连续性被打断；进入病房后调阅患者 CT/MR 影像，传统带宽不足导致日渐完善的 AI 阅片、AI 辅助诊断、影像组图深度诊断等业务无法顺利开展，系统及大文件加载长达数分钟，查房和诊疗效率大打折扣——这两大痛点本质上都指向同一个问题：移动中的高带宽需求。与此同时，门诊和病房点位扩展时，传统布线需重新穿墙打洞，施工周期长达数天，还可能影响正常诊疗秩序，严重制约了医院布局的灵活调整。

因此，如图 18 所示零漫游与万兆到病房一体化方案在医疗领域得到了极大的应用。配合 Wi-Fi 7 技术实现毫秒级无感切换，移动查房全程零掉线，护士 PDA 数据上传成功率提升至 99.99%，无需再因网络重连而重复操作，单次查房耗时平均缩短 30%以上；医生在床边即可流畅调阅全部影像资料，并利用 AI 辅助诊断及高清可视化功能，查房效率与医患沟通质量均得到质的提升。在急救场景，CT/MR 影像的秒级调阅直接关系到黄金抢救时间的把握——网络卡顿不再是效率问题，而是生命安全问题。以太全光将万兆带宽延伸至诊室和病房，影像调阅从平均 3 分钟缩短至 5 秒以内，可确保急救数据零等待、零丢失，为生命救援争分夺秒。

案例：某大学附属儿童医院采用 Wi-Fi 7 无感漫游方案，内网、外网带宽分别达到 400M，平均时延 7.8ms，PDA 漫游 0 丢包；移动护理车业务稳定运行，查房效率得到极大提升；外网独立组网，不干扰内网，支持 50 终端并发上线 0 掉线，0 卡顿。影像秒级加载，单次调阅时间从平均 3 分钟缩短至 5 秒以内，CT/MR 数据可实时进行 AI 三维重建，同时，系统界面切换及加载也因低时延、0 丢包变得顺畅。此方案有效解决了医疗场景中实时阅片的网络技术卡点，医生诊断效率显著提升。

（2）物联感知融合部署

当前，医院物联网应用日益丰富，但 Wi-Fi、蓝牙、RFID 等多协议独立建网导致“烟囱式”架构，部署复杂、建设成本高昂，运维压力大；此外，患者体征数据传统采集方式耗时耗力，容易出现数据采集不及时或数据不准的情况，影响医生对病情进展的判断，更可能在突发状况下延误应急响应；同时，在 AI 技术赋能下，患者生理数据、医嘱信息与执行数据可实现高效融合，支撑精细化病情分析与风险预警，而传统多通路、多系统分散汇总的数据模式，弱化了 AI 分析赋能效果。

如图 18 所示，通过多协议合一的 AP 统一接入与管理物联终端，显著简化架构、建网成本降低 50%，运维压力同步减轻。以此为基础，实现医疗固定资产自动盘点与物资轨迹管理；同时借助网络物联能力利用轻量级手表或毫米波雷达无感采集患者心率、血压、呼吸等数据，结合监护仪、麻醉剂等传统物联终端的数据，自动整合并上传至平台，

实现 7×24 小时不间断监测，一旦发现异常立即告警，医护人员第一时间响应。

案例：某省人民医院采用“三网合一”方案，通过部署多协议融合的物联AP实现RFID、Wi-Fi的一体化部署；成功落地婴儿防盗、贵重资产管理、移动输液、医护人员定位等功能、大大提升医院服务质量和运营效率。此外，病房内部署毫米波雷达设备，无需接触患者即可实时感知其呼吸和心跳引起的微弱起伏，自动提取心率、呼吸频率等生命体征数据，并通过无线网络上传至医院平台，实现7×24小时不间断的“无感守护”，一旦发现异常，系统立即告警，医护人员第一时间响应，有效避免了突发风险，患者安全得到充分保障。

（五）万兆 AI 赋能智能制造

1.趋势与要求

根据《中华人民共和国国民经济和社会发展第十五个五年规划纲要》及《“人工智能+制造”专项行动实施意见》的战略部署，要加快制造业数智化转型，推动规上企业（“规模以上”企业：年主营业务收入在 2000 万元以上）应转尽转，全面融入数智化进程，加速设备更新、工艺升级和质量提升。这意味着“十四五”提出的 70%数字化、网络化目标将进一步升级为全覆盖要求。

智能制造正朝高度数字化、网络化和智能化发展。工业物联网、AI、5G、边缘计算等技术融合应用，推动企业向 AI 质检、预测性维护、柔性产线、个性化定制和绿色低碳演进。网络作为基础底座，联

接人-机-料-法-环，支撑数据采集、流转与价值变现。构建网络需将各类生产要素联网，满足上层应用对联接的需求，推动研发、生产、运营转型升级，保障稳定生产与柔性制造。

2.典型应用

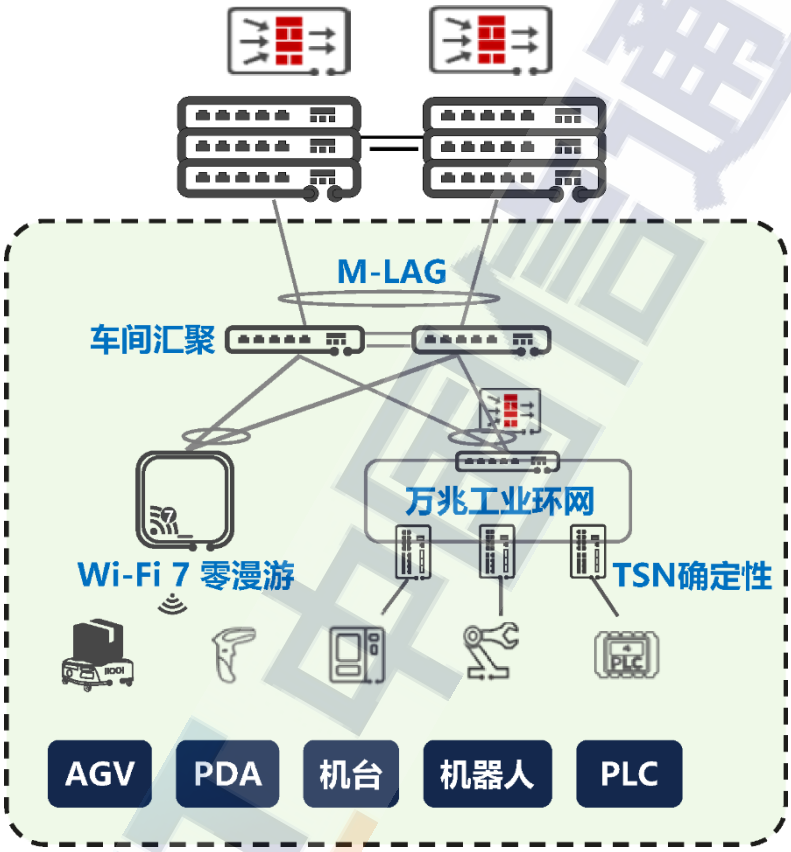

图 19 智能制造网络架构图

（1）高可靠生产

制造企业的稳定量产依赖高可靠生产网。如图 19 制造生产网架构图所示，三大关键技术可协同构筑这一底座：万兆大带宽为高清机器视觉 AI 质检与数字孪生提供无阻塞传输动脉，满足产线爆发式带宽需求；TSN 确定性网络则以微秒级抖动的超低时延，为多轴协同赋予精准“时间基准”，确保产线上数十个机械臂的动作严格同步，避

免因微秒级时间偏差导致的碰撞或产品缺陷；高可靠工业环网作为最后防线，能在网络故障时 20ms 以内实现快速倒换，将业务中断压缩至工业协议容忍阈值内，避免产线骤然停机。三者协同，构建出“既宽又快、且稳能自愈”的融合网络底座，为 7×24 小时不间断的高价值生产铸就数智化韧性。

案例：某半导体制造工厂，一颗芯片的制程有1000多道工序，会涉及大量的原材料、能源表计和配方数据等，其生产过程由计算机集成一体化制造（CIM）系统进行AI协同调度。半导体制造过程如中断30分钟，因原材料浪费、返工等经济损失会高达¥5000万。通过架构级可靠M-LAG网络冗余机制和链路级以太网环保护倒换（ERPS）技术，为产线的稳定量产提供了稳定的生产环境，保障了业务不中断。通过高品质万兆IT和OT融合一张网，实现数据互联互通，承载数字孪生海量数据，确保网络可视化、智能化管理，实现智慧工厂建设。

（2）柔性制造

柔性制造市场年复合增长率达 20%，产线需依据订单快速重构，AGV 跨区搬运成为常态。传统有线布线因物理束缚与机械磨损，难以适应动态工位调整，业务中断风险陡增，同时 AGV 在跨区漫游过程中容易因为漫游掉线触发安全停机，导致任务中断，严重影响产线节拍。

全无线 Wi-Fi 7 零漫游 AI 网络方案：其单用户极限速率超 4.5Gbps，可承载高清视觉回传；同时基于 AI 算法在底层实现的“零感”调度，

支持多 AP 同频点虚拟为一个“大 AP”，确保 AGV 在高速移动中漫游丢包率≤1‰，连续丢包数不超过两个，切换时延控制在 20ms 以内，从而保障 AGV 零趴窝，真正实现生产业务“零感”不中断。

案例：某制造工厂，AGV 移动速度 1-2m/s，1000 平方米的车间内部署了 50 台的 AGV 小车用于生产部件的移动搬运等工作，每天因网络丢包重启导致的 AGV 停机达 12 次。通过引入全无线 Wi-Fi 7 零漫游 AI 网络方案，将 AGV 漫游丢包率降低至≤0.2‰，AGV 实现不停车运行，生产效率提升 35%。

（六）万兆 AI 赋能智慧酒店

1.趋势与要求

当前酒店业正由数智化 AI 驱动，聚焦智慧体验升级与安全合规双主线。

在智慧方面，酒店正在从“自助入住”迈向 AI 驱动的“主动智能服务”，智慧终端已成标配，网络也由“高速连接”演进为支撑海量物联终端和 AI 应用的“超大规模智能承载网”。

在安全方面，住客隐私保护已上升为不可逾越的法定红线。2025 年 4 月 1 日正式施行的《公共安全视频图像信息系统管理条例》中明确规定，酒店必须对客房进行日常管理和检查，若未尽到检查义务导致房间被安装偷拍设备，须承担相应法律责任。传统人工巡检频次低、死角多，难以有效应对日益隐蔽的偷拍手段，构建一套持续运行、高效检测的技术排查体系，已成为酒店依法合规经营的必选项。

上述趋势对酒店网络提出了两大核心诉求：一是搭建万兆网络底

座，保障酒店业务的高效稳定运行，二是基于融合感知、融合物联、网络探测等高阶能力，实现酒店的智慧化升级，如图 20 智慧酒店架构图所示。基于以上这些核心诉求，推出以下典型应用解决方案。

2.典型应用

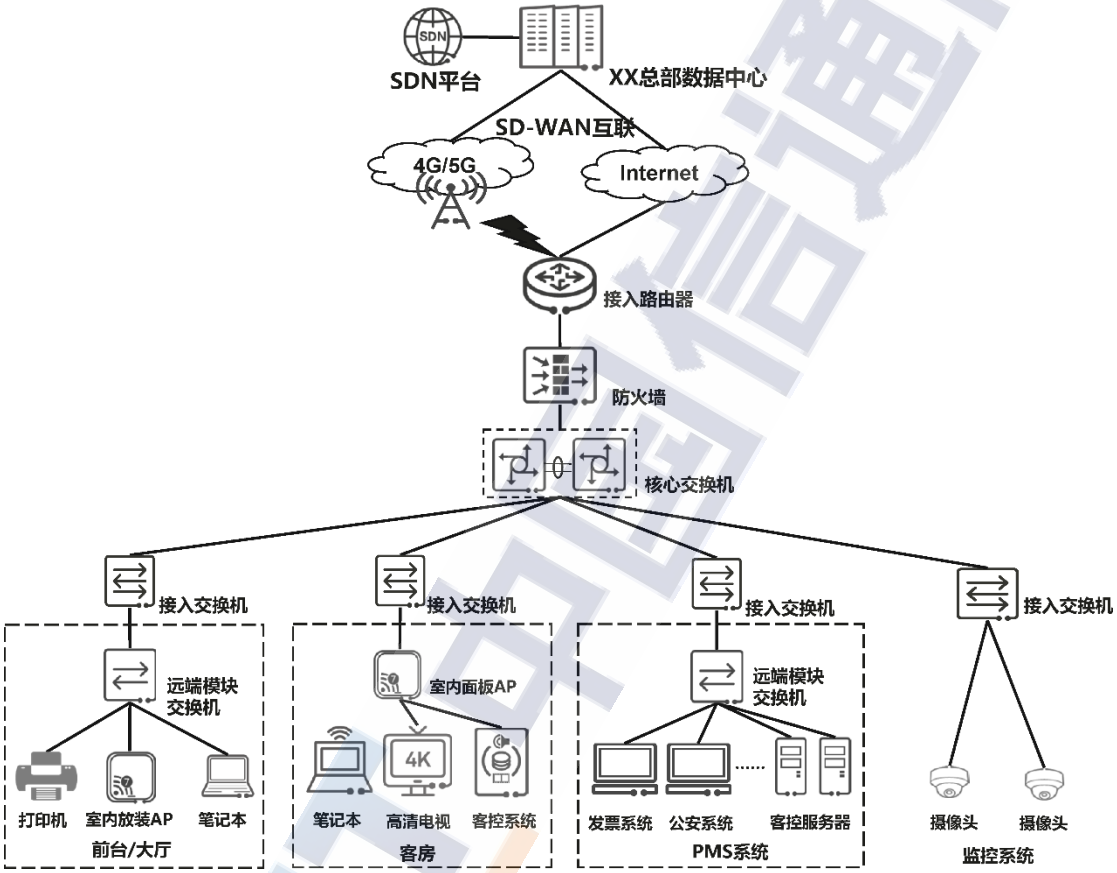

图 20 智慧酒店网络架构图

（1）智慧客房

智慧客房不仅能提供全屋智能的沉浸式体验，还能助力酒店节能降本、打造差异化卖点以提升房价，已成为酒店升级的必然趋势。然而，传统智能化改造每个客房需要额外部署大量硬件，施工涉及大量布线，单间改造成本高周期长，让众多酒店望而却步。

酒店网络通过融合物联与融合感知能力，提供轻量化的智慧客房

改造方案。在感知侧，AP 复用 Wi-Fi 信号探测环境动态变化，并基于 AI 算法对信号特征进行实时处理，有效抑制环境杂波干扰，实现人员存在精准判断，联动能源系统调节灯光、空调等，实现超 20%的节能效率。在物联侧，AP 通过内置软件化客房控制单元（RCU）和 IoT 芯片，实现各类智能终端可通过无线快速组网接入，有效压缩硬件投入、缩短施工周期，实现轻量化快速改造。

案例：某酒店在智慧客房改造初期，拟采用传统方案，每间客房需部署2~3个红外传感器以检测人员存在，同时配置RS-485总线、独立客房RCU等硬件，施工涉及大量布线作业，原计划改造周期长达2~3个月，改造成本超过50万。后期酒店改采极简智慧客房方案，通过AP的融合感知能力和融合物联能力，省去硬件加装与重新布线环节。客房改造周期亦由原计划的2~3个月压缩至1个月以内，硬件采购与施工改造成本整体减少约20万元。改造后，系统可联动酒店能源管理平台，综合能耗下降约30%，投资回收周期缩短至18个月。

（2）安心酒店

尽管法规已明确酒店对客房偷拍设备的检查义务，但传统人工抽检方式存在三大短板：频次低、死角多、依赖肉眼识别，对 SD 卡存储型、蜂窝回传型等不发射 Wi-Fi 信号的偷拍设备几乎无能为力。

酒店网络应构筑主动防御体系，利用 AP 内置的 AI 探测引擎对客房内潜在隐藏摄像设备进行 7×24 小时不间断巡检，覆盖 Wi-Fi 传输型、SD 卡存储型及蜂窝网络回传型等多类型偷拍设备。一旦探测到可疑设备，AP 即主动上报后台管理系统，运维人员可快速定位并

及时移除，将传统抽检的被动响应升级为全天候主动防御。

案例：某酒店部署了具备防偷拍检测功能的 Wi-Fi 7 AP。该 AP 内置的 AI 探测引擎支持 7×24 小时不间断主动探测，可对客房内潜在的不同类型的隐藏摄像设备进行持续巡检。实测表明，对比传统人工抽检因频次低、死角多，漏检率通常超过 60%等问题，该方案检测漏检率控制在 5%以内，酒店运维人员可据此快速响应、精准定位并及时移除隐患。

（七）万兆 AI 赋能智慧零售

1.趋势与要求

随着零售企业持续加快门店扩张和数智化升级，新店建设、网络运维及智能设备接入面临更高要求。企业希望门店能够实现快速开局，网络部署随门店同步上线，满足“开店即营业”的业务需求；同时，面对成百上千家门店和有限的 IT 运维人员，需要通过远程统一管理和智能运维降低运维成本，提升管理效率；此外，电子价签、视频监控、自助收银、智能货架、IoT 传感器等设备快速普及，传统多网并行架构复杂、建设和维护成本高，亟需构建统一承载、多业务融合的一体化网络，为零售业务持续创新和规模化发展提供高效、可靠的网络底座。基于以上这些核心诉求，推出满足“快速开局，远程运维，多网融合”三大核心诉求的智慧零售解决方案，如图 21 所示。

2.典型应用

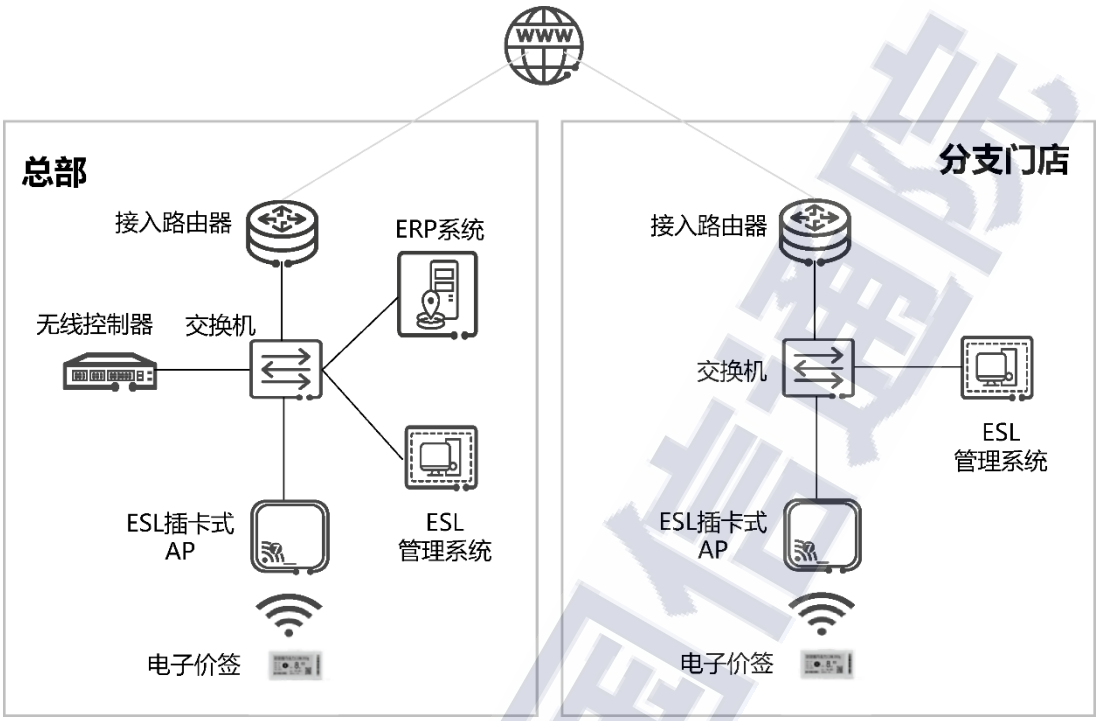

图 21 智慧零售网络架构图

（1）智慧门店

随着零售门店持续推进数智化升级，电子价签、自动拣货机器人、智能货架、环境传感器等智能终端不断增加。由于不同终端对通信距离、功耗和带宽需求不同，传统方案往往需要部署多套独立网络，不仅建设复杂，还增加了后期运维成本。

针对此场景，AP 具备物联网融合能力，支持 Zigbee、蓝牙、RFID 等主流物联协议，并兼容 PCIe 插卡、物联沉底、USB 等多种扩展方式，实现一张网络统一承载多种物联业务，避免重复建设，降低部署和运维成本。同时，AP 支持容器化开放架构，可根据门店业务需求适配更多的增值应用，持续扩展电子价签、AI 巡店、资产管理等智能业务，打造统一、开放、易扩展的门店物联网络。

案例：某超市促销打折季，前一天晚上需要集中更改数千纸质价签，费时费力，效率低下。因此客户高层决定部署新的电子价签方案，解决传统纸质价签更改耗时费力的问题。通过部署Wi-Fi 7 + IoT电子价签融合方案，实现TCO降低30%，结合AI智能运营能力，系统可基于库存周转率、竞争对手调价、天气预报等因子自动生成动态调价建议，经店长确认后一键推送至全场价签，将传统的“人力改价”升级为“算法定价”，大幅提升门店数字化运营效率。

（2）门店极简运维

零售行业门店遍布全国、终端设备数量庞大，IT 运维人手不足的矛盾日益突出。传统运维采用被动响应模式，故障引发门店投诉后才开始排障，且高度依赖现场处理，运维效率低下。

新建门店业务上线更快网络设备通电即可自动联网，不需要专业人员到现场逐台配置。总部提前准备好不同类型门店的网络配置，新店开业时一键下发即可完成部署。无论是新开一家店，还是批量拓展数百家门店，都能做到业务开到哪里，网络就同步开通到哪里，真正实现“当天装、当天用、当天营业”。

门店覆盖范围广，基于 AI 智能运维能力，实现网络风险主动识别、智能根因分析和自动优化，助力网络从“被动运维”向“主动运维”升级。网络运行状态一目了然，故障发生后能够快速定位位置、分析原因，大部分问题远程即可处理，无需频繁派人到店，大幅降低运维成本，提升门店网络运维效率。

案例：某全国性快餐连锁品牌在全国拥有 4000 多家门店，门店开通需要数天之久，多分支门店解决方案可以做到配置统一下发，设备即插即用，单门店开局时间降至分钟级满足了零售企业快速扩张的需求，结合软件定义广域网（SD-WAN）多链路技术，确保断网不停业、收银不中断，保障门店营收连续性。多分支门店运维采用 AI 智能运维方案，结合全网状态可视化、AI 主动预警、远程排障与本地自愈的方式，极大提升运维效率，将故障恢复时间从天级缩短至分钟级，无需工程师上门。

五、展望

面向未来，随着 AI 技术与模型能力持续迭代演进，Agentic AI 将会以数字人的形式替代当前人工，重构 AI 的业务流。据 Gartner 预测，到 2028 年，预计 33%的企业应用将会内置 Agentic AI 的能力，15%的业务决策将由 Agent 自主完成；到 2029 年，50%以上的知识工作者将按需通过创建 Skill 和智能体来解决复杂的任务。作为 IT 基础设施的重要一环，园区网络的运维模式也将被 Agentic AI 重塑。传统的以命令行界面（CLI）、图形用户界面（GUI）为入口的运维模式，将会完全被以自然语言交互的模式颠覆。Agent 将取代传统网络专家进行 7×24 小时不间断值守，而人工将转向业务流的监控、关键策略的审批及端到端业务流的优化。

与此同时，伴随着芯片的演进，更强的算力及千亿级参数以上的模型部署于端侧，AI 终端的出货量占比将逐步提升，云边端协同计算将成为主流。智能眼镜、具身机器人等新型设备的大规模接入，将

引入多模态感知数据以支撑模型计算，使园区网络尤其是无线接入带宽将面临巨大的压力，整体网络流量预计增长 10~100 倍。此外，多 Agent 协同控制业务形态的出现，要求网络在保障高带宽承载的同时还需要提供确定性的时延。因此，未来的园区网络需在大带宽、低时延及高并发调度方面持续发力。

未来网络正实现从“单一通信”向“通感算一体”分布式传感底座的跨越。在应用层面，泛办公场景可依托 AP 共站部署，实现人员跌倒即时预警与区域热力分析；智慧安防依托射频指纹与异常检测能力，实现无摄像头隐私防护；工业领域结合 Wi-Fi 微功耗传能与星闪物联技术，达成 10 毫秒极低时延下的万物永续互联与免电池极简运维。在技术层面，网络通过 GHz 连续频谱采样和高集成大规模感知阵列，融合边缘轻量化感知大模型，赋能厘米级空间分辨率与毫米级微动感知能力，在极致提升感知颗粒度的同时，确保数据本地化处理的绝对隐私。

然而，企业 Agent 的广泛应用也引入了新型攻击面。AI 可自主挖掘 0 DAY 漏洞、自动构建攻击链，将网络对抗从小时级加速至秒级，并开启 7×24 小时持续攻击，导致传统基于“人”和“边界”的安全模型彻底失效，倒逼企业针对每个 Agent 和连接实施语义级细粒度管控。随着数字世界与物理世界的孪生融合，全息多维感知技术使得隐私防护范围从传统数据延伸至生物特征、行为轨迹、空间位置及生活习惯等全维度信息。面对网络空间与物理时空的深度重叠，需构建高安全、强隐私的 Agentic 自主治理架构，以应对数实融合带来的

全新安全挑战。

面向未来，园区网络与 AI 已形成深度共生、双向驱动的演进关系。网络通过通感算一体化升级，为 AI 模型的持续迭代提供高确定性的多模态数据输入与高性能传输保障；同时，AI 原生技术也全面融入网络的运维与安全架构，驱动网络实现高程度的自主治理。这种技术范式的深度融合，将从根本上重塑企业 IT 基础设施的战略价值，成为企业数智化转型的核心驱动力。

缩略语

缩略语	英文全称	中文全称
AC	Access Controller	无线控制器
AES	Advanced Encryption Standard	高级加密标准
AGV	Automated Guided Vehicle	自动导引运输车
AI	Artificial Inelligence	人工智能
AP	Access Point	无线接入点
BSSID	Basic Service Set Identifier	基本服务集标识符
CIM	Computer Integrated Manufacturing	计算机集成一体化制造
CLI	Command Line Interface	命令行界面
CSI	Channel State Information	信道状态信息
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DPD	Digital Pre-Distortion	数字预失真
ECC	Elliptic Curve Cryptography	椭圆曲线加密算法
EDR	Endpoint Detection and Response	端点检测和响应
ERPS	Ethernet Ring Protection Switching	以太网环保护倒换
FTM	Fine Timing Measurement	精细时间测量
GUI	Graphical User Interface	图形用户界面
HSR	High-availability Seamless Redundancy	高可用无缝冗余协议
IoT	Internet of Things	物联网
KRACK	Key Reinstallation Attack	密钥重装攻击
MAC	Media Access Control	媒体访问控制
MACsec	Media Access Control Security	媒体访问控制安全
mGE	Multi-Gigabit Ethernet	多速率以太网
M-LAG	Multichassis Link Aggregation Group	跨设备链路聚合组
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism	基于模格密钥封装机制

缩略语	英文全称	中文全称
PA	Power Amplifier	功率放大器
PCIE	Peripheral Component Interconnect Express	高速串行计算机扩展总线
PDA	Personal Digital Assistant	个人数字助理
PLC	Programmable Logic Controlle	可编程逻辑控制器
PoE++	Power over Ethernet Plus Plus	增强型以太网供电
PQC	Post-Quantum Cryptography	抗量子密码
PRP	Parallel Redundancy Protocol	并行冗余协议
QAM	Quadrature Amplitude Modulation	正交幅度调制
QoS	Quality of Service	服务质量
RCU	Room Control Unit	客房控制单元
RFID	Radio Frequency Identification	射频识别
RSSI	Received Signal Strength Indicator	接收信号强度指示
SDN	Software defined Networking	软件定义网络
SZTP	Secure Zero Touch Provisioning	安全零配置部署
TCO	Total Cost of Ownership	总拥有成本
TSN	Time Sensitive Networking	时间敏感网络
TTL	Time To Live	生存时间
USB	Universal Serial Bus	通用串行总线
UWB	Ultra Wideband	超宽带
WAPI	WLAN Authentication and Privacy Infrastructure	无线局域网鉴别与保密基础结构
WLAN	Wireless Local Area Network	无线局域网
WPA2	Wi-Fi Protected Access 2	Wi-Fi 保护访问第二版
WPA3	Wi-Fi Protected Access 3	Wi-Fi 保护访问第三版
ZTP	Zero Touch Provisioning	零配置部署

中国信息通信研究院 技术与标准研究所

地址：北京市海淀区花园北路52号

邮编：100191

电话：010-62300120

传真：010-62300123

网址：www.caict.ac.cn