

高品质万兆AI园区建网技术 白皮书



目 录

1 园区业务的趋势和挑战	5
1.1 无线化趋势	5
1.2 数智化趋势	6
1.3 融合化趋势	7
1.4 绿色化趋势	8
1.5 安全化趋势	8
2 高品质万兆园区的概念和内涵	12
2.1 高品质万兆园区架构和定义	12
2.2 自治网络	15
2.2.1 自治网络定义	15
2.2.2 自治网络关键技术	15
2.2.2.1 数字孪生网络	15
2.2.2.2 智能决策	16
2.2.2.3 自动部署	16
2.2.3 关键指标	16
2.3 万兆超宽	17
2.3.1 万兆超宽定义	17
2.3.1.1 万兆无线	18
2.3.1.2 万兆有线	18
2.3.2 万兆超宽关键技术	22
2.3.2.1 连续组网	22
2.3.2.2 智能漫游	22
2.3.3 关键指标	23
2.4 泛在接入	24
2.4.1 泛在接入定义	24
2.4.2 泛在接入关键技术	24
2.4.2.1 无线通感一体化	24
2.4.2.2 短距通信技术	25
2.4.3 关键指标	25
2.5 确定体验	26

- 2.5.1 确定性体验定义26
- 2.5.2 确定性体验关键技术26
 - 2.5.2.1 优先级确定26
 - 2.5.2.1.1 应用优先级26
 - 2.5.2.1.2 用户优先级26
 - 2.5.2.2 带宽确定27
 - 2.5.2.3 时间确定27
 - 2.5.2.4 高可靠性27
- 2.5.3 关键指标27
- 2.6 绿色节能28
 - 2.6.1 绿色节能定义28
 - 2.6.2 绿色节能关键技术28
 - 2.6.2.1 设备级节能28
 - 2.6.2.2 网络级节能28
 - 2.6.2.3 智能楼宇协同29
 - 2.6.3 关键指标30
- 2.7 全域安全30
 - 2.7.1 全域安全定义30
 - 2.7.2 全域安全关键技术31
 - 2.7.2.1 资产管理31
 - 2.7.2.2 终端合规准入和微分段32
 - 2.7.2.3 链路安全33
 - 2.7.2.4 网安智能防御34
 - 2.7.2.5 韧性可信34
 - 2.7.3 关键指标35
- 3 高品质万兆 AI 园区的典型应用37**
 - 3.1 高品质万兆 AI 园区在教育 37
 - 3.1.1 趋势与要求37
 - 3.1.2 推荐组网架构37
 - 3.1.3 智慧办公38
 - 3.1.4 智慧教室39
 - 3.1.5 智慧宿舍40
 - 3.2 高品质万兆 AI 园区在政府 41
 - 3.2.1 趋势与要求41
 - 3.2.2 推荐组网架构42
 - 3.2.3 政务大厅42
 - 3.2.4 移动办公43
 - 3.3 高品质万兆 AI 园区在金融 44
 - 3.3.1 趋势与要求44

3.3.2 推荐组网架构	44
3.3.3 智慧办公	45
3.3.4 智慧网点	46
3.4 高品质万兆 AI 园区在医疗	47
3.4.1 趋势与要求	47
3.4.2 推荐组网架构	47
3.4.3 智慧门诊	48
3.4.4 智慧病房	49
3.4.5 智慧手术室	49
3.5 高品质万兆 AI 园区在制造	50
3.5.1 趋势与要求	50
3.5.2 推荐组网架构	50
3.5.3 高可靠融合生产网	51
3.6 高品质万兆 AI 园区在零售	52
3.6.1 趋势与要求	52
3.6.2 推荐组网架构	52
3.6.3 智慧零售门店	53
3.7 高品质万兆 AI 园区在酒店	54
3.7.1 趋势与要求	54
3.7.2 推荐组网架构	54
3.7.3 智慧酒店	55
4 产业展望	57
4.1 产业展望	57
A 缩略语	58

1 园区业务的趋势和挑战

园区是城市的基本单元，是人类生产生活的主要场所，是数字经济发展的主要载体，是实现绿色低碳转型的关键靶点。以 5.5G、人工智能、数字孪生等为代表的前沿技术加速发展，驱动园区进一步向全面智能演进，并创造新场景和新应用。近年来，业界对智慧园区进行了深入的探索和实践，智慧园区的发展已经进入深水区。

园区覆盖了绝大部分工作生产场景，80%以上的 GDP（Gross Domestic Product，国内生产总值）和 90%以上的创新在园区内产生，园区网络作为园区业务的重要载体和必要工具，园区业务发展趋势可推导出园区网络演进趋势，园区业务发展具有以下趋势。

1.1 无线化趋势

园区接入到网络中的无线终端主要包含两类，一类是智能终端，例如个人电脑（Personal Computer，PC）、手机等；另一类是物联终端，例如：智能门锁、电子价签、未来还会有眼镜、手表和裸眼 3D 大屏等。

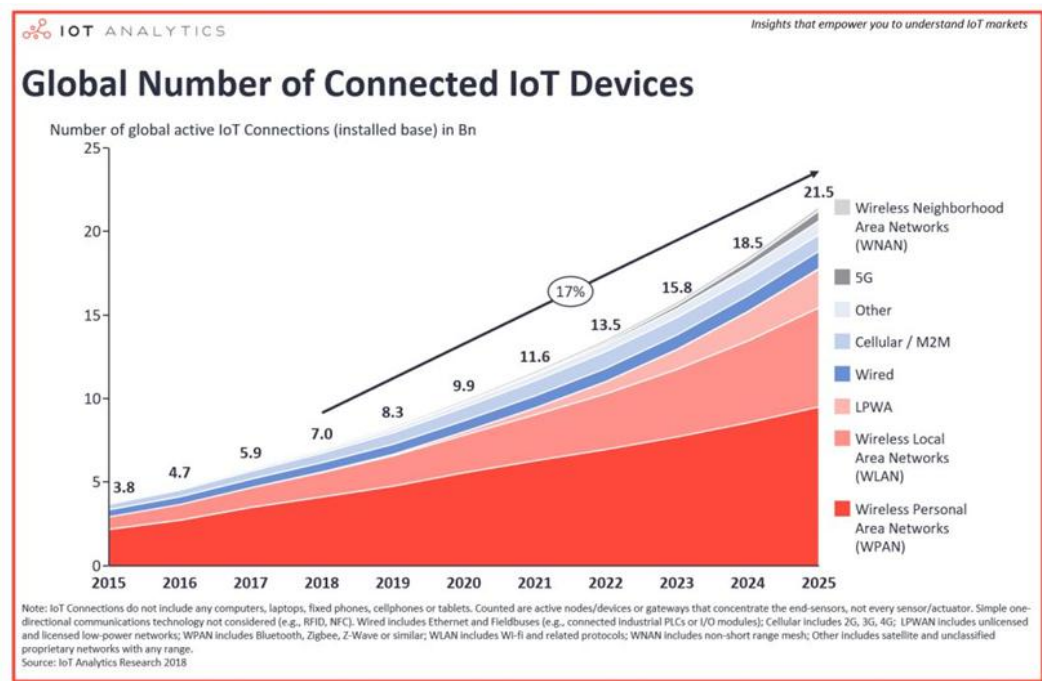
1. 接入到网络中的智能终端和物联终端的数量近十年来（2015 年~2025 年）增长近 2.5 倍，根据 Gartner & ABI Research 权威机构统计和预测，近 3 年个人终端数量增长 3-5 倍，促使园区网络的接入终端密度从"单一用户单设备"迈向"单用户多设备协同"时代，对网络并发连接能力提出更高要求，需要园区提供高性能高并发的无线 Wi-Fi 网络。
2. 对于物联终端，IoT Analytics 的分析师团队分析得出，目前全世界的联网设备数量已经超过 170 亿，除智能手机、平板电脑、笔记本电脑或固定电话等智能终端连接之外，物联终端的数量已达到 70 亿，这一数据得到了广泛的认可，并反映了物联网技术在全球范围内的快速发展，其中 80%的物联终端以无线接入的方式连接到网络中，而且仍然在以 17%的年增长率快速增长。

表 1-1 终端对园区网络的核心挑战

挑战维度	数据支撑	网络需求
终端密度	人均 3 - 5 台终端 (2025)	高并发接入能力（如 Wi-Fi 7/8）

挑战维度	数据支撑	网络需求
流量压力	AR/裸眼 3D 等新型终端普及	万兆级无线带宽 & 低延迟
物联终端多	70 亿物联终端设备（全球）	多协议兼容（Wi-Fi/BT/Zigbee/RFID）
网络管理	80% IoT 依赖无线 + 无线物联终端 17%年增长率	自动化运维 & 终端智能识别

图 1-2 全球物联设备连接方式与增长率示意图



1.2 数智化趋势

园区基础设施独立建设，系统孤立、数据割裂，无法满足园区数字经济产业可持续发展需要。未来的园区应部署高品质、适度超前的新型物联感知网以及网络基础设施，依托万兆联接的网络，真正开启园区全局感知、万物智联的新时代。

到 2030 年，全球联接总量将突破 2000 亿，完全进入到万兆联接的时代。新一代 Net5.5G 联接技术助力园区实现精准定位、高速网络全覆盖以及无边界信息传递。同时，园区未来将通过部署泛在物联感知设备，收集监测基础设施的各项运行状态数据，基于海量数据和 AI 大模型构建园区数字孪生，进而打造全面感知、人机协同、实时在线的智能化园区，使得园区具有自学习、自诊断、自决策和执行能力。通过数字技术和机器人等智能设备的结合，构建无人值守、自动控制、自适应学习等能力，全

面提升园区建设和运营效率。进而实现对用户行为及偏好的自主感知，实时响应，满足用户个性化需求。

1.3 融合化趋势

传统园区采用子系统割裂的建设模式，导致安防、能效、会议等系统互相割裂、独立运行，进而出现数据孤岛、业务协同难、管理效率低下、系统维护费用高等问题：

- 资源碎片化：办公、生产、安防、物联等系统独立建网重复投资，布线冗余难于维护，CAPEX、OPEX 增加 40%以上。
- 运维复杂化：多网并行引发策略冲突、故障定位困难，平均修复时间（MTTR）超过 4 小时。

图 1-3 资源碎片孤岛

楼宇基础设施																																						市政基础设施
信息化应用系统								信息设施系统								建筑设备管理系统										公共安全系统												
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	
公共 服务	智能卡应用	物业管理	信息设施运行管理	信息安全系统	访客系统	停车场库	信息接入系统	布线系统	移动通信室内信号覆盖系统	卫星通信系统	用户电话交换系统	无线对讲系统	信息网络系统	有线电视及卫星电视接收系统	公共广播系统	会议系统	信息导引及发布系统	时钟系统	建筑设备监控系统	建筑能效监管系统	冷热源系统	空调通风系统	给排水系统	照明系统	电梯扶梯系统	供电系统	环境监控系统	供暖通风系统	火灾自动报警系统	安全技术防范系统	应急响应系统	安防监控中心	视频监控	出入口控制系统	入侵报警系统	路灯管理系统	井盖检测系统	

通过网络架构升级，整合垂直业务网络，实现“一网多用、多能”，显著提升网络资源效率与业务无缝对接能力。数智化驱动下，园区正从静态空间演变为具有自我进化能力的“有机生命体”，通过 AI 深度协同感知数据与网络资源，实现资源自动调节、业务需求预判及瞬时响应，为创新业务提供水电般无处不在的智能连接。海量设备与传感器打破信息孤岛，构建智能会议/楼宇/园区生态系统，其核心依赖实时数据采集、分析与流转的基础设施能力。在此过程中，数据作为核心资产的全生命周期管理催生两大融合变革：

1. 通感协同网络优化：人员分布热力图等感知数据动态驱动网络切片带宽调整；
2. AI 赋能自治网络：基于业务优先级自动调度感知与网络资源；最终实现新业务上线周期从月级缩短至小时级，并支撑 OPEX 降低 30%的核心目标。

ABI Research 预测，架构升级与数智化融合转型不仅可实现 OPEX 降低 30%的核心目标，更将推动企业 WLAN 市场在 2028 年达到 145 亿美元规模。

表 1-2 传统架构与升级架构关键指标对比

指标	传统架构	升级架构	提升幅度
业务上线周期	3-6 个月	2-8 小时	98% ↑
资源利用率	30-40%	70-85%	100% ↑

指标	传统架构	升级架构	提升幅度
故障修复时间	4-12 小时	<1 小时	85% ↑
运维人力投入	高（需专职团队）	低（自动化为主）	60% ↑

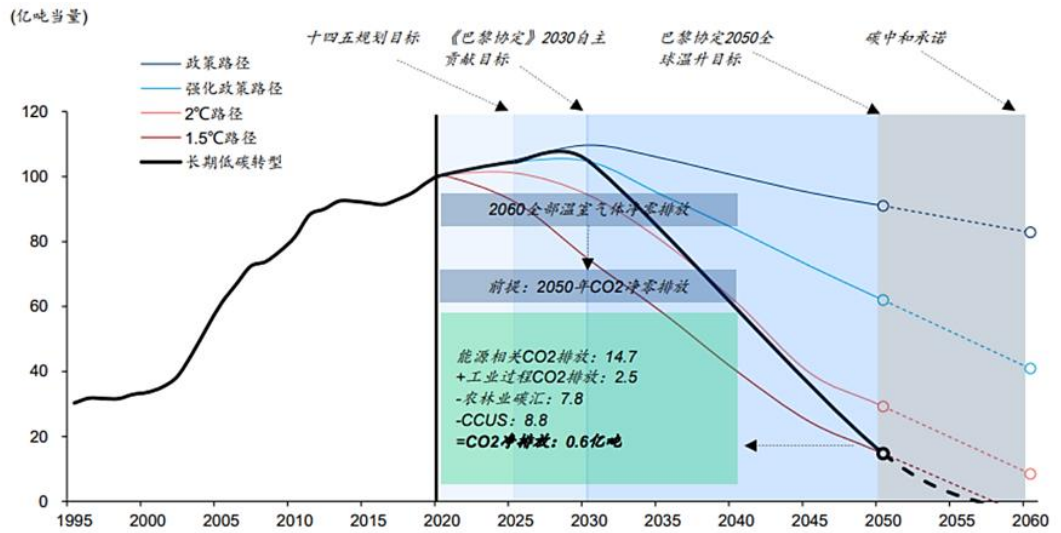
1.4 绿色化趋势

园区占城市碳排放的 60%以上，是“碳达峰/碳中和”目标的主战场。在这一目标引领下，绿色化转型已成为园区的核心战略，正在从单一节能改造向系统性零碳运营演进。

零碳/近零碳园区作为“碳达峰/碳中和”战略部署的重要空间载体，将顺应绿色化、清洁化、循环化等绿色低碳发展的政策要求，鼓励在园区的建设、运维和管理的各个阶段积极开展零碳转型探索。通过比特管理瓦特，园区亟需在数字化发展和“碳达峰/碳中和”目标中找准平衡点：既要满足园区智慧化所需的物联及网络设备等电力需求，又要采用数字技术促进园区能源结构清洁化、能源管理高效化、生产生活绿色化。

园区生产领域的零碳转型是一项多维复杂的系统工程，需要园区生态的协同，提升信息基础设施和管理服务、产业智慧化和高质量发展及园区-城市智慧化融合；基于网络助力，探索契合自身特色的绿色低碳建设路径，科学落实动态零碳目标。

图 1-4 零碳转型规划和目标



1.5 安全化趋势

物联化和多网融合（5G/Wi-Fi、云边协同）彻底打破了传统基于物理隔离的“城堡式”安全边界，导致攻击面呈指数级扩张，安全威胁无处不在。同时网络安全已从

“支撑系统”跃升为“核心生产力要素”，其重要性等同于业务本身。因此园区网络亟需构建覆盖“终端接入-网络传输-业务数据”全链条、全场景的安全防护体系，形成融合网络环境下的多维纵深防御。

表 1-3 安全业务场景与典型风险

业务场景	具体场景/风险点	典型风险	关键特征/挑战
终端接入	IoT 设备： - 部署在公共场合易被私接仿冒 - 摄像头、传感器等固件未更新（存在高危漏洞，CVSS$\geq$9.0） - 工业 PLC/SCADA 等使用默认密码或弱密码 - 车载系统 OTA 升级机制存在漏洞	- 勒索病毒感染（导致设备停摆、数据加密） - DDoS 僵尸网络（设备被控发起攻击） - 关键基础设施停摆（工控设备遭破坏） - 车辆控制权劫持（危及人身安全）	- 海量异构设备：种类繁多，台账不清晰，管理困难。 - 生命周期长/更新难：固件更新滞后或无法更新，漏洞多。 - 物理暴露性：设备常部署在无人值守或开放环境，易被私接仿冒。 - 安全基线缺失：默认配置不安全，缺乏统一安全标准。
	智能终端： - 远程办公设备（笔记本、手机）通过不安全的公共 Wi-Fi 接入企业网络 - BYOD 设备未安装合规安全软件、未受 MDM 管控即访问敏感业务	- 勒索病毒传播（通过受感染终端进入内网） - 敏感数据泄露（设备丢失或被窃取） - 内部网络横向渗透跳板	- BYOD 管理难题：设备所有权在个人，安全控制弱。 - 接入环境复杂：通过不可信网络接入企业核心资源。

业务场景	具体场景/风险点	典型风险	关键特征/挑战
网络传输	网络边界模糊化： 5G、Wi-Fi 6/7 与有线网络深度融合 - 云数据中心、边缘节点、终端设备间数据频繁交互（东西向流量） - 微服务架构导致内部网络通信复杂度剧增	- 横向渗透攻击（攻击者在网络内部肆意移动） - APT 攻击隐匿传播（利用复杂网络拓扑隐藏行踪） - 勒索软件跨域感染（从 IT 域蔓延到 OT 域或不同云环境） - 网络嗅探与中间人攻击（在传输链路窃听或篡改数据）	- 物理隔离失效：5G/Wi-Fi 混合组网、云边协同、多云互联导致传统“内/外”边界消失。 - 东西向流量激增：服务器/应用/微服务间通信流量巨大且复杂，传统边界防火墙难以有效监控。 - 加密流量挑战：大量加密流量（如 TLS）使得深度检测难度增加。
业务数据	数据流动性与暴露面增大： - 敏感数据在终端、边缘节点、云端及不同业务系统间频繁流动 - 数据存储在混合云、边缘节点甚至终端设备 - 应用微服务化导致数据访问权限管理复杂	- 中间人攻击窃取数据（在传输环节截获敏感信息） - 钓鱼渗透获取凭证（用于非法访问数据） - 内部数据泄露（恶意内部人员或配置错误导致） - 勒索软件加密数据（导致业务中断和数据资产损失） - 违反数据合规性要求（如 GDPR、CCPA）	- 数据无处不在：分布在终端、边缘、云端，流动路径复杂。 - 多环境存储：数据存储在公有云、私有云、本地数据中心、边缘设备等多种环境。 - 权限管理复杂：跨网络、跨环境、跨应用的细粒度权限控制难度高。 - 数据生命周期管理：数据的创建、存储、使用、传输、销毁各环节均需保护。

据 Gartner 预测，到 2026 年，60%企业将因安全缺口导致业务中断而强制部署零信任架构。融合网络的安全本质是业务连续性的基石——唯有将安全能力植入网络基因，方能在数字化浪潮中构筑“智能”与“可靠”并重的未来园区。

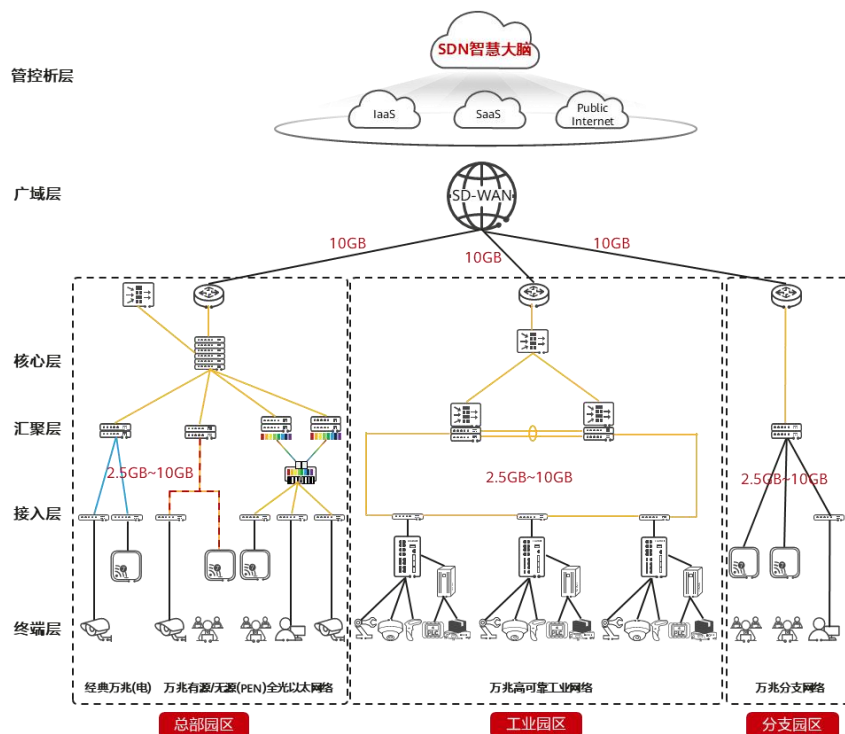
2 高品质万兆园区的概念和内涵

2.1 高品质万兆园区架构和定义

高品质万兆园区网络物理架构

如图所示，园区网络包括终端层、接入/汇聚/核心网络层、广域层和管控析层。终端层包括各种智能终端和物联终端。接入层包括有线/无线网络接入设备。汇聚/核心层由盒式或框式交换机组成。广域层由路由器和防火墙组成。管控析层包括 SDN 控制器和分析器，是网络管理的大脑。

图 2-1 高品质万兆园区网络物理架构

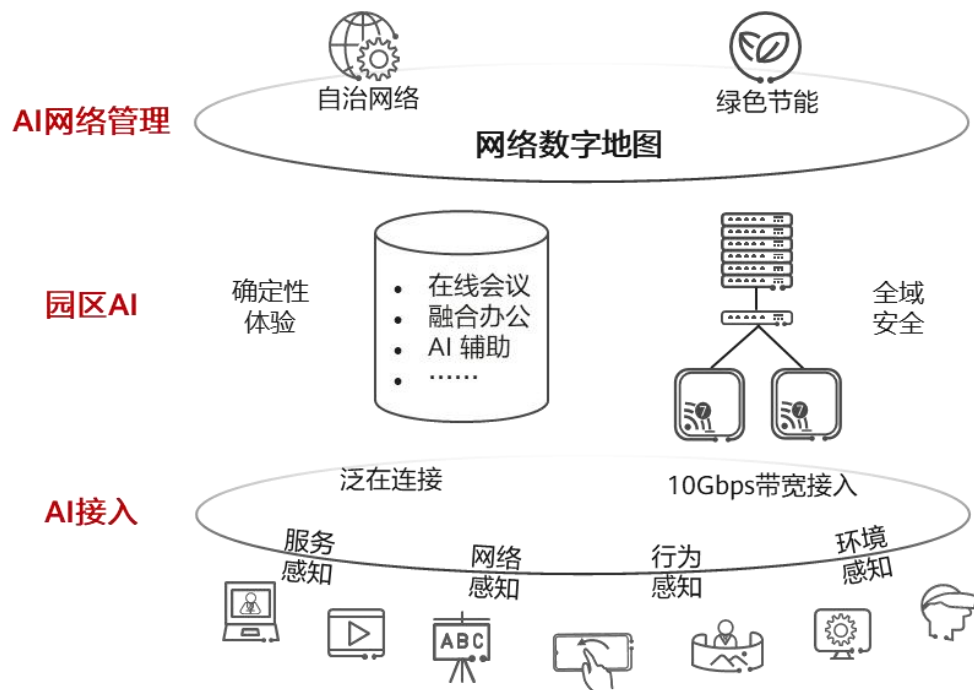


- **终端层**：园区办公、生产等各种接入终端，包括智能终端和物联终端等。

- **接入层：**接入终端的网络设备层，提供 2.5GE~10GE 的万兆接入能力，包括 Wi-Fi 7 无线接入、2.5GE/10GE 有线接入等方式。
- **汇聚层：**接入设备到核心设备之间的网络设备层，是园区当前比较活跃和丰富的一层，支撑万兆接入能力，包括以太电和以太光两种主流方案。
- **核心层：**一般会部署核心交换机，对接防火墙、路由器、汇聚层交换机等，具有高性能、高密度、高扩展性等特征，承担整个园区的业务。
- **广域层：**提供园区出口路由能力。在多分支园区场景下，提供分支园区高性能互联能力。同时具备网络安全防护能力，确保园区网络设备、业务的安全性。
- **管控析层：**作为园区软件定义网络（Software defined Networking, SDN）“大脑”承担着园区网络设备管理和控制，园区业务分析和保障等关键职责，是智能化园区的中枢。

面向未来的 AI Campus 逻辑架构和关键能力

图 2-2 面向未来的 AI Campus 逻辑架构和关键能力



AI for Network: 升级 AI 大脑的网络管理

通过引入大型模型和自然语言翻译等新技术，帮助网络向 L4 自动驾驶演进。一方面，园区网络可以为 AI 提供更多的信息，如终端、服务和流量、位置和环境等，帮助 AI 提升整体能力，比如可以利用感知信息实现智能楼宇感知节能，打通楼宇管理系统联动空调、灯等智能开关控制；另一方面，大型模型可以实现自动化检查和维护，支持设备级、网络级和应用级的实时可见性，用户和应用级的实时旅程回放，并实现分钟级的问题定界定位。网络智能代理通过故障分析模型自动分析故障根本原因，实现 90% 的无线故障检测和自闭环。

Campus for AI: 升级 AI 应用的网络体验

随着终端 AI 代理的普及，AI 代理如何安全快速的使用成为了网络的关键挑战。基于 AI 应用智能识别和保障技术，AI 应用会话可以实现毫秒级确定性延迟和 1E-9 丢包率，满足新 AI 终端、代理和服务（如具身智能、AI 操作系统等）的高质量高标准网络诉求。结合基于 AI 的流量收集和识别分析能力，网络可以为不同用户和服务的 AI 应用提供差异化体验服务，为 AI 提供实时服务能力。

同时，园区还可以通过无线和有线链路的物理加密，为 AI 终端和代理提供全面安全保障。

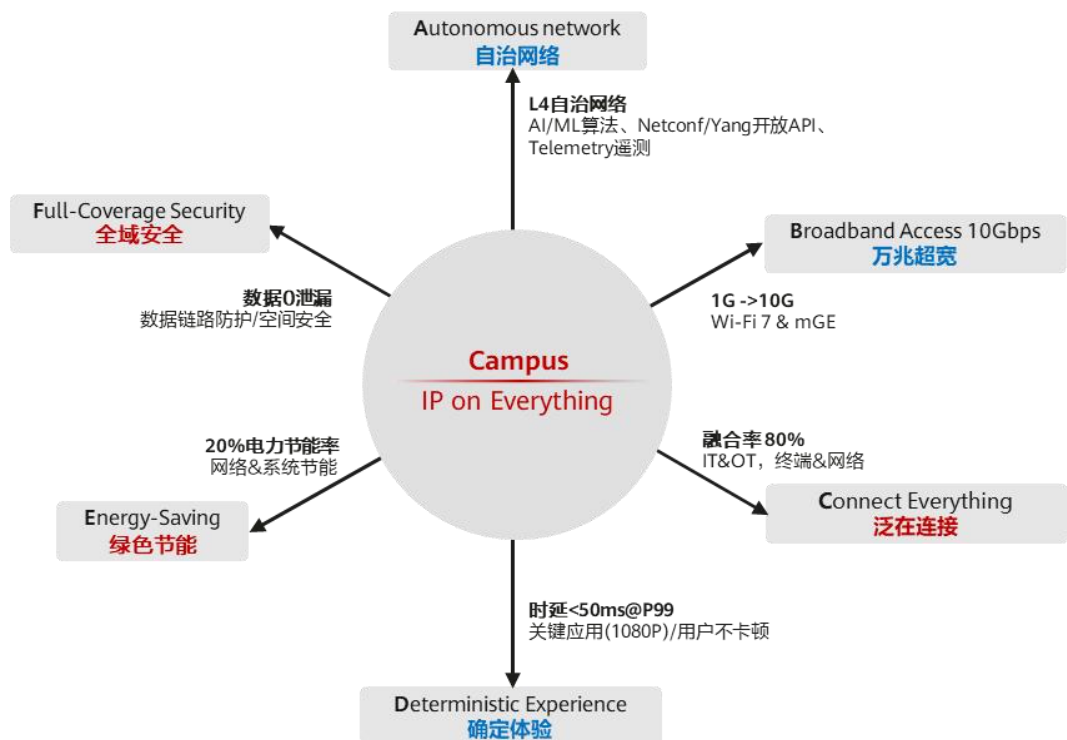
AI for Access: 通过 AI 技术升级终端管理能力

各种类型的终端是园区网络的主要服务目标，也是威胁的关键来源。因此，在网络接入层实现可见性、可管理性和安全控制是校园网络的关键挑战。AI 技术可以解决终端类型识别和行为控制，实现自动化配置和保护策略等功能。此外，空间感知可以进一步实现从连接到空间的全面安全保障。

AI 驱动的校园关键技术

根据业务场景和能力，园区网络可以定义为六个关键技术方向。

图 2-3 AI 驱动的校园关键技术



1. **网络自治：**L4 自动驾驶网络可实现网络管理高度自治，通过网络智能体和大模型的引入，管理系统具备自主分析与自主决策能力，可基于园区网络的实时状态进行运行态势预测，并基于客户输入的业务意图主动的完成业务闭环管理。比如远程免上站开局 100%成功，非上站类故障 100%自闭环，80%无线问题可实现自动检测闭环，AI 智能化给出用户体验评分。数字地图实现一站式管理网、安、用户和终端一图可视，质量可视可定位。

-
2. **万兆超宽：**Wi-Fi 7 和 8 技术带动接入带宽向 10GE~100GE 升级，Wi-Fi 可实现 10 米高性能覆盖，利用融合调度、空间复用和智能变焦天线容量提升 60%~80%，高可靠连续组网 0 丢包，极简承载网变三层架构为一层实现一台设备一张网。
 3. **泛在连接：**WLAN+X 无线泛在连接，为园区丰富的接入连接提供了关键技术基础。Wi-Fi 远距离通感一体感知（大于 15 米），通过 FTM 精准定位、CSI 和毫米波精准感知，可实现感知安全和感知节能等方案；Wi-Fi IoT 从分布式无源到集中式，可实现 10 米半径共站部署，支撑资产管理、医疗和零售和工业等行业场景的物联融合进一步简化，满足下一代工业生产提供柔性制造、安全生产的要求。
 4. **确定体验：**随着 AI 终端、具身智能、智能制造等场景的普及，园区网络亟需提供确定性网络体验保障。通过智能应用识别可基于流量特征识别音视频、云桌面、协同办公等关键应用，通过智能全流调度可基于整网端到端切片和端网协同实现 AI 和 XR 业务卡顿率<1%，通过智能全流分析可支持百万级全流质差分析，应用级旅程回放和整网可视等能力，通过 VIP 用户和终端业务保障，可支持 VIP 随时随地优先接入，确定性时延< 50ms 和带宽保障的效果，同时还可支持 VIP 主动关怀，体验实时评估和故障及时预警等能力。
 5. **绿色节能：**节能已经成为业界共同的使命，网络设备既要解决自身能耗的问题，又要考虑解决园区整体节能的问题。利用 AI 潮汐预测、新的节能协议标准以及芯片智能休眠，可实现网络设备节能 20%；利用无线感知技术可实现 Bit 控制 Watt，通过感知人员变化控制空调、照明等设施，实现园区整体节能 20%。
 6. **全域安全：**园区场景人员活动密集，安全建设薄弱，往往成为整个系统的最薄弱环节，比如勒索病毒很容易通过园区内部设备进行传播，因此我们需要重视和提升园区网络安全体系，包括零信任接入 ZTNA/ZTL，通过 AI 加持实现入网零信任，实时 95%以上的异常行为检测；通过无线和有线链路层加密技术实现端到端数据零泄漏，特别是无线空口链路层防窃听技术可以从根本上解决无线安全隐患；通过 CSI 等 Wi-Fi 空间感知和检测技术，可实现秒级入侵检测和异常设备如摄像头的检测；通过系统的设备安全防护架构和态势感知实现端侧和网元侧系统安全防护。

2.2 自治网络

2.2.1 自治网络定义

自治网络是指利用网络的数字孪生，通过海量数据实时采集，把物理世界的网络在数字空间中重建，通过大数据和 AI 的智能分析来呈现和实时分析业务质量情况，通过 AI 算法主动优化，通过自然语言交互，人机对话，智能决策闭环网络故障和体验问题，从而提升网络服务质量，缩短故障处理时间。自治系统的关键技术包括数字孪生网络、智能决策和自动部署，这些能力共同推动系统向高度自动化和智能化发展。

2.2.2 自治网络关键技术

2.2.2.1 数字孪生网络

数字孪生网络(Digital Twin Network)是以数字方式构建物理网络实体的虚拟孪生体，且可与物理网络进行实时交互映射。网络的数字孪生体作为物理网络设施的数字镜像，与物理网络具有几乎相同的网络拓扑、业务及流量数据模型，是真实物理网络全生命周期、多维度的精细化副本，支持对历史的追溯和回放，快速实现故障问题的分析，

同时现网实施的调整、维护、优化等变更操作，都可以先在数字孪生网络中进行充分的试验和验证，并通过其反馈来不断的评估、修正、优化操作方案，最大限度降低对真实网络带来的冲击。

数字孪生网络通过 Telemetry 等技术，实时海量获取设备、用户、应用、终端实时信息，把物理世界的网络在数字空间中重建，系统清晰呈现各种网络和业务的状态信息。

2.2.2.2 智能决策

智能决策（Intelligent decision-making）是系统通过网络演算、仿真验证等技术实现策略及应用的实时仿真，模拟网络设备资源要求及网络连通性影响等信息，再基于智能决策系统，通过历史数据不断优化修复策略，能够自动检测、诊断并修复故障，选取最优方案对网络参数进行调整优化，持续不断优化网络，从而提供最优质的网络服务。

例如利用机器学习基于故障特征库在秒级采集的大数据仓库中自动关联分析、挖掘，并结合专家经验识别异常；而同时，海量大数据的汇集也给通过机器学习从海量数据中发现未知关联和因果关系，创造了条件。解决人工识别时间长，依赖个人经验的缺点，机器学习通过对海量数据持续学习，从而识别出复杂的业务模式、构建动态基线预测数据趋势、挖掘未知的关联关系，从而识别潜在故障和根因定位。

运维人员可通过自然语言和系统交互，快速了解系统整体健康状态，并自动分类出紧急需要处理和需要关注的任务，同时，资源语言融入到整个交互框架和流程中，用户可以跟智慧伴行的对象进行交互，下发配置，提供智能问答、智能联动、快速提供报表，知识协同功能。

2.2.2.3 自动部署

自动部署是指系统基于意图理解、配置综合等技术根据业务需要提取网络资源要求，根据不同的场景进行网络模型建模，自动推荐出不同场景下的标准组网，实现网络的免规划、免设计，并且通过网络校验、自动部署、智能容错等能力实现网络的自动化快速部署。自动部署关键技术：

1. ZTP 开局和设备自动发现：设备支持 ZTP（Zero Touch Provisioning，零配置部署），具备邮件开局、U 盘、及 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）选项等多种开局模式，通过远程配置，现场即插即用，能够快速完成分支部署。
2. 模板化开局：可以基于自定义模板，或者通过预置模板自动生成相关的站点网络配置，通过站点模板的固定参数和每个站点的差异化变化参数的组合，批量生成站点配置，达到快速生成站点网络配置并进行部署的目的。
3. 意图开局：用户可以通过自然语言表达配置意图，描述期望目标网络到达的状态，然后经过意图验证与综合求解两个过程后，得出具体的网络配置数据后，自动下发到设备。

2.2.3 关键指标

要实现网络完全的自治，必然是一个长期的过程，不可能一蹴而就。因此存在部分自治，限定条件的自治，高度自治和全自治等阶段。当前发展主要在限定条件自治和高度自治的发展阶段，相关建议的能力如下：

表 2-1 自治网络关键指标

分类	推荐值（高度自治）	基础答标值（限定条件自治）
数字孪生网络	支持园区网络边界（广域网，数据中心）的连接状态分析，可快速界定问题	支持园区网络内的连接状态分析
	支持基于应用质量（丢包和时延和抖动）进行实时监控和问题原因分析	支持网络设备连接，用户和终端状态和上下线、离线问题的查看和原因分析
智能决策	自动生成网络瓶颈的分析和优化方案	基于设备类问题的定位，如带宽不足，端口故障等
	基于应用的历史数据的分析自动推荐优化保障方案	关键键应用质差分析和给出修复建议
	无线射频自动优化，无线 VIP 用户高体验保障	无线干扰源的发现和定位，质差分析给出故障建议
	基于现网状态和业务意图的最优配置自动化生成	业务下发后的自动测试验收
	支持自然语言交互，快速反馈网络状态和故障问题和处理建议或自动处置	图形化界面显示故障问题和处理建议
自动部署	支持自然语言交互的意图开局，基于 VIP 用户的体验保障自动下发 基于业务意图的组网方案自动生成，比如基于 SLA 保证的网络方案推荐业务意图保障指标和方案的自动生成	支持 ZTP
	根据场景进行最佳实践推荐和场景化网规，基于历史数据的组网和参数的自动生成和推荐网络规划事前仿真和评估，预置专家经验的合规校验	支持模板化开局

2.3 万兆超宽

2.3.1 万兆超宽定义

万兆超宽是以万兆接入为目标的下一代接入超宽演进趋势，是指园区内的用户终端利用无线或有线的大带宽和高并发接入能力实现高速网络连接，满足园区中新兴应用对网络带宽、时延和并发的诉求。关键技术包括无线网络提供的 Wi-Fi 7 接入、连续组网技术以及智能漫游技术；有线网络提供的以太全光接入技术，包括有源以太光技术和无源以太光技术等。

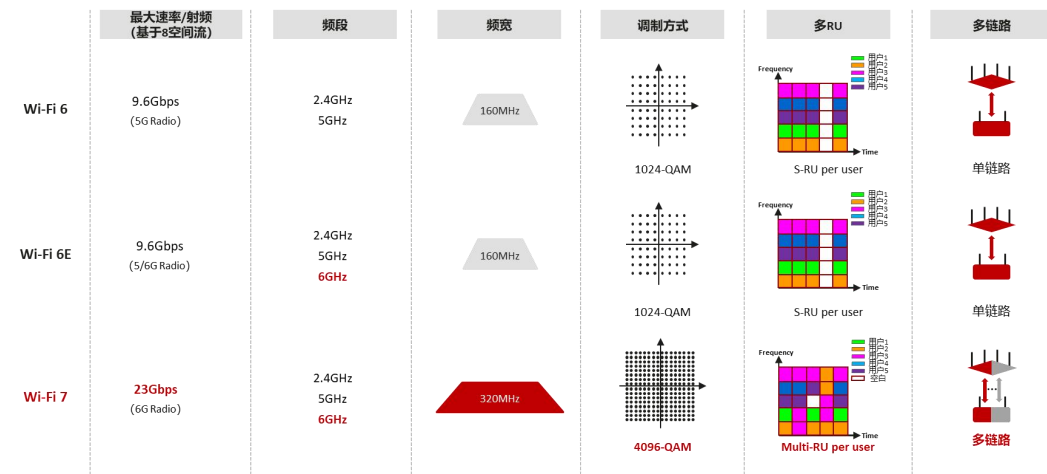
园区联接 (Connectivity)作为联接物理世界和数字世界的桥梁，构建覆盖园区全域、高带宽、低时延、高可靠、可扩展的融合通信网络基础设施。强调以全 IP 化为特征，实现有线无线一体化（Wi-Fi 6/7, 5G）、物联感知网络（NB-IoT, LoRa 等）的统一接入和管理。联接层为终端数据的实时采集、平台指令的快速下达、云边协同提供畅通无阻的“高速公路”，是万物互联的基础保障。

2.3.1.1 万兆无线

万兆无线，是指利用 Wi-Fi 7 协议的改进以及通过 AP 之间协同工作提供的高带宽、高并发以及无感漫游的能力，满足园区网络中新兴应用对网络带宽和时延的诉求。

Wi-Fi 7 标准通过引入 6GHz 频段、320MHz 频宽、4096-QAM 调制方式、Multi-RU、Multi-Link 等技术，将 Wi-Fi 网络的吞吐率提升到 23Gbit/s，并且为用户提供低时延的接入保障，高品质万兆园区需要部署 Wi-Fi 7 网络来提升网络使用体验。

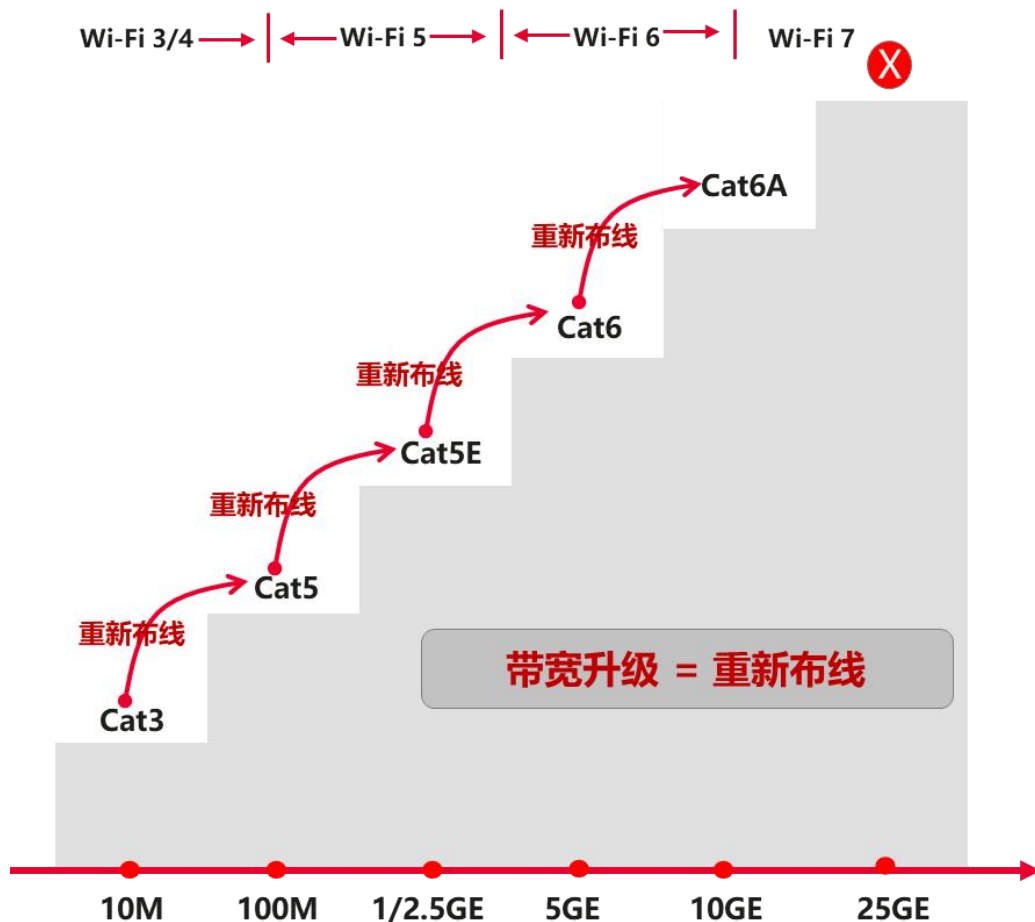
图 2-4 Wi-Fi 标准对比



2.3.1.2 万兆有线

万兆有线，是指有线终端及无线网络上行带宽升级到 10GE。配套网络提速存在线缆更新问题，GE 升级 2.5G 速率可以利用旧线缆并配套 Wi-Fi 7 上行端口基础速率，优先推荐该模式。对于新建网络，可采用全光以太技术直接演进至 10GE 光网络。

图 2-5 电缆与 Wi-Fi 代际演进关系



电到光演进存在一个过渡期，因此业界提出一个经典网络，两个创新网络的概念。图 2：经典网络架构，包括网络管理系统，2.5GE 交换机和 Wi-Fi 7 AP。2.5GE 接续 GE，可提升网络带宽容量 20%。图 3：融合光电复合缆长距供电和高速接入能力的 2.5GE 网络架构；图 4：融合无源彩光技术的极简 10G 全光网络；10GE 光纤高速入室，弱电机房无源化，安全可靠，满足未来业务演进。

图 2-6 2.5GE Wi-Fi 7 传统网络

"2.5GE + Wi-Fi 7" 替换 GE,
提升容量20%.

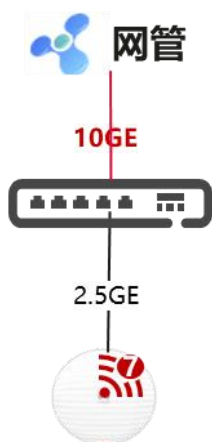


图 2-7 融合长距供电的光电复合缆 2.5GE 网络

2.5GE 光电复合缆入室,
同时满足Wi-Fi 7接入和供电

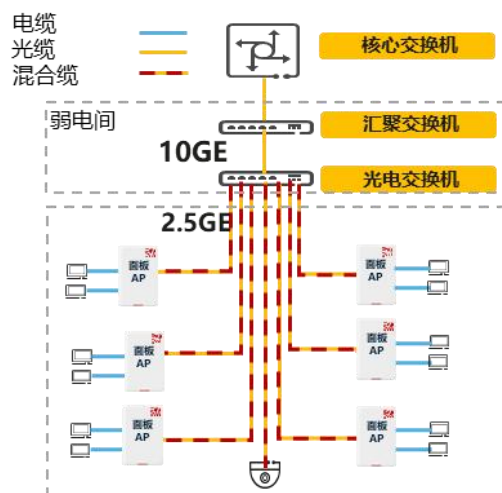
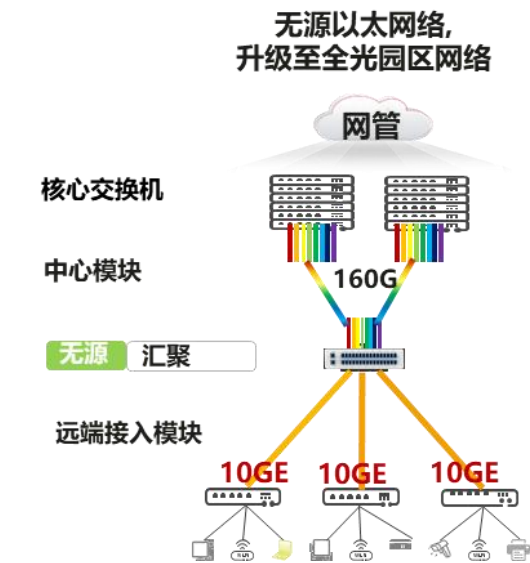


图 2-8 极简无源 10GE 全光网络



光电复合缆可满足长距供电同时提供高速接入能力，由于一体化集成，可以大大简化网络部署，如图所示

图 2-9 光电混合电缆和光模块构成

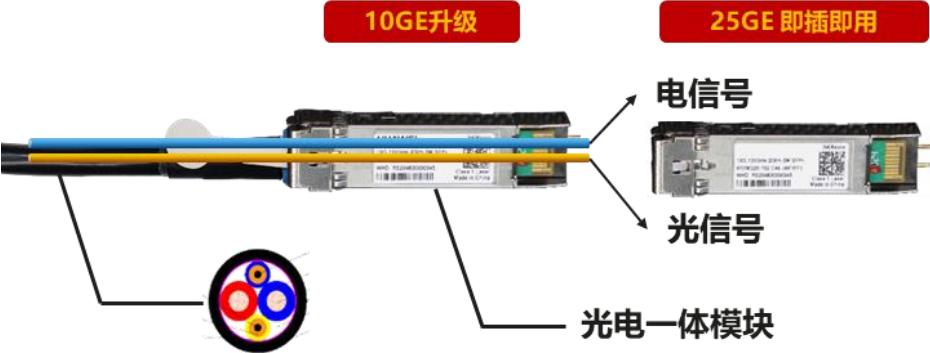


表 2-2 光电混合缆关键支持能力

线缆规格	线径	PoE 供电距离 (15.4W)	PoE+供电距离 (30W)	PoE++供电距离 (60W)
光电混合缆- 17AWG	6.2mm	1280m	500	250
光电混合缆- 21AWG	5.7mm	500m	200	100
光电混合缆- 24AWG	4.4mm	200m	100	50

*AWG（American Wire Gauge，美国线规）是用于表示导线直径的标准单位。AWG 数值越小，导线直径越粗，载流能力越强。

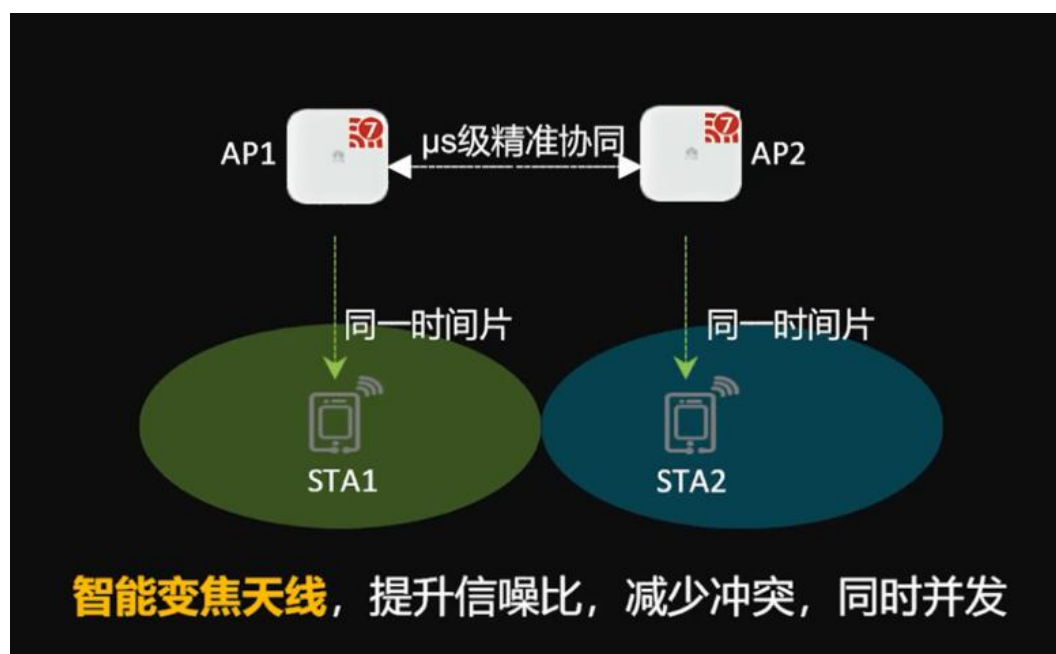
2.3.2 万兆超宽关键技术

2.3.2.1 连续组网

连续组网，是指在多 AP 组网的情况下，保证 WLAN 网络可以提供无缝的连续的信号覆盖的同时，保证用户在无线网络中可以获得最佳的业务体验。连续组网中的关键技术包括智能天线和多 AP 协同工作两个方面。

连续组网通过 AP 射频芯片之间 μs 级别精度的数据同步，形成 AP 分组和优先级。当 AP 抢占到信道之后协商成为主 AP，主 AP 根据分组信息，通知从 AP 进行调整智能天线的覆盖角度，并且同步发送数据报文。最终使得多个 AP 可以在同一信道上工作，从而显著提高频谱效率，提升系统的容量。

图 2-10 智能天线和多 AP 协同工作示意图



2.3.2.2 智能漫游

智能漫游是指通过网络 AI 能力对终端漫游行为进行画像，进而对终端进行差异化漫游引导，解决传统漫游过程中出现的粘性终端、信道扫描时间长、终端漫游兼容性差等漫游问题，提升终端漫游体验。智能漫游的关键技术包括终端识别、终端画像、终端质量数据学习以及漫游牵引等。

智能漫游由终端主动漫游变为网络侧引导漫游，优化漫游切换时机，缩短漫游时间；同时基于每类终端配置个性化漫游参数，最大程度消除协议兼容性和终端实现差异带来的负面影响。

图 2-11 智能漫游切换示意图



2.3.3 关键指标

万兆超宽的园区网络，应达到如下要求。

表 2-3 万兆超宽的园区网络关键指标

分类	指标项	卓越	优秀
带宽	单用户极限速率	$\geq 3.5\text{Gbps}$	$\leq 3.5\text{Gbps}$
	3 个 AP 80M 同频组网+18 个终端总吞吐	960Mbps	700Mbps
	带宽独享	支持万兆	支持千兆
并发	4K 高清视频路数	60 路	40 路
	高密彩光端口	96/PCS	80/PCS
长距接入	长距 PoE++能力	$\geq 250(\text{米})$	$\geq 200(\text{米})$

2.4 泛在接入

2.4.1 泛在接入定义

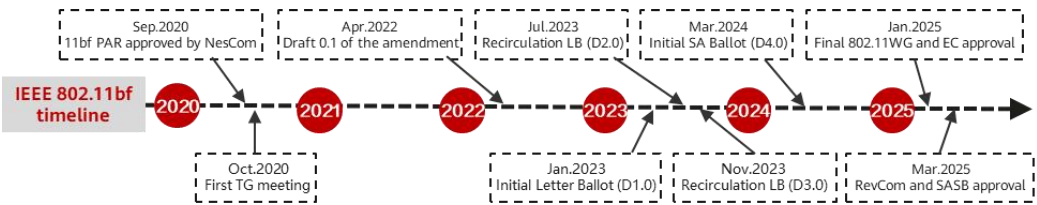
园区内的一些行业新兴应用不仅需要高品质无线连接，而且需要提供广泛的接入场景，包括无线高精度定位，无线的通感一体化感知，和 IoT 物联融合等能力。利用趋同的无线基础设施（如高频段/大规模天线），同步提供高品质通信（如 Wi-Fi 物联）与环境感知（如定位/成像），突破单一通信功能，实现物理空间的无缝感知与服务覆盖。

2.4.2 泛在接入关键技术

2.4.2.1 无线通感一体化

IEEE（电气电子工程师学会）在 802.11bf 中明确定义基于 WLAN（无线局域网）通感一体产业演进方向，通过具备 WLAN 感知能力的站点（STA）接收的无线信号来确定特定环境中目标特征的技术，进一步通过无线局域网与园区数字平台等深度组合，实现对园区内环境和设备的实时监控、智能分析和快速响应，为智慧园区的建设和发展提供了强有力的技术支撑。

图 2-12 802.11bf 标准时间线



WLAN 作为园区的泛在感知载体其商用优势凸现在两大方面：

- 广泛存在与成本优势：疫情后全球广泛接受移动分布式办公、业务上云等作业方式，WLAN 将持续成为园区中最广泛覆盖的信息系统，其作为感知末梢对物理世界进行数字化收集、处理和分析天然具有极大的相对优势。
- 隐私保护与数据安全：我们身处的数字时代中隐私保护和数据安全重要性日益凸显，传统视觉感知与 WLAN 等技术的融合感知可以在有效保护隐私安全和信息安全的前提下更加有效的做到低成本覆盖和多维精准判断。

Wi-Fi 感知应用涵盖房间级存在检测（10 米）、AI 辅助定位追踪（2~5 米）、亚米级肢体活动识别，厘米级生理体征监测（呼吸/心跳）及医疗级成像等场景，提供一种有效且经济的无线感知技术手段。相较于红外/毫米波方案，其通感一体架构通过免布线、多系统融合显著降低部署与运维成本。

图 2-13 Wi-Fi 感知应用场景

应用场景	技术手段	KPI性能指标或建议频段
人体存在检测	人体不同状态对应时间域上的信道CSI波动，识别是否存在人体。包括移动，静止场景。	最大覆盖范围：10m~15m 距离分辨率：0.5m~2m 距离精度：<0.2m
活动识别	基于CSI提取多普勒谱、目标移动速度CSI幅度变化等	大尺度活动：Sub-7GHz 小尺度活动：60GHz
目标定位及跟踪	The fingerprinting-base(常用): 基于数据库定位和跟踪 Geometric model-base methods: 基于多参数联合估计，提升多径信道场景定位跟踪性能，性能受限于天线数和带宽	距离分辨率：0.5m 距离精度：<0.2m
体征检测	估计信道CSI幅度、相位变化	心跳检测：60GHz

2.4.2.2 短距通信技术

园区终端 (Terminal)园区终端作为智慧园区的感知端，对园区的信息及监测起着重要的作用。通过部署各种传感器和监控终端，如传感器、探测器、摄像头等，实时监测园区内的温度、湿度等环境信息，发现潜在的安全风险。终端层的关键趋势是智能化（内置边缘计算能力）、IP 化（支持网络直接接入）、多功能集成化。它们是数据的源头和智能指令的执行末端，其广泛覆盖和智能化程度直接影响整体感知精度和响应速度。

- 1. 星闪（NearLink）：中国原生标准的颠覆性创新，覆盖车、工业控制、全屋智能等多个应用领域，联盟成员超 1200 家，芯片出货量 2024 年 8500 万片（2025 年破亿），覆盖问界 M9、享界 S9 等 20+车型，2025 年产品品类将达 500 种 136。
- 2. 蓝牙：新增信道探测技术，提升室内定位精度（亚米级）；与星闪互补提供“星闪+蓝牙”动态切换方案，降低跨设备干扰。但其在定位精度（1-3 米）和时延仍落后星闪/UWB。
- 3. UWB：厘米级高精度定位王者。技术原理：纳秒级窄脉冲（带宽≥500MHz），通过 TOF（飞行时间）测距与三边定位算法实现 10 厘米级精度。主要用于工业自动化、仓储物流等场景，具有安全抗中继攻击的优势。
- 4. NFC：安全近场交互的不可替代性，核心特性：10cm 内近场通信，防窃听与未授权访问，适合金融支付、门禁系统。可简化蓝牙配对流程（“一碰连”），提升消费电子用户体验。

2.4.3 关键指标

表 2-4 泛在接入关键指标

指标项	卓越	优秀
通讯/感知方式	WiFi 7，通感一体	独立的 WiFi、红外/毫米波传感器
通信技术	星闪+蓝牙	蓝牙

指标项	卓越	优秀
点位数量	不增加	增加传感器覆盖点位（1个/10~15 m ² ）
布线	现有网络布线	增加传感器独立布线（RS485等）
系统	多系统合一	多套系统相互独立
运维难度	一套系统运维	多系统独立运维

2.5 确定体验

2.5.1 确定性体验定义

随着数字化经济的深化和产业智能化升级，园区作为经济活动与创新的核心载体，网络需求已从传统的“连接能力”向“体验质量”跃迁，而传统网络“尽力而为”的数据传输方式是“不确定”的，经常发生数据丢包、传输抖动等“意外”。确定体验是通过优先级确定、带宽确定、时间确定、高可靠性来提升用户的网络体验，满足不同场景对网络质量的要求。

2.5.2 确定性体验关键技术

2.5.2.1 优先级确定

优先级确定包含确定性的应用转发优先级，和确定性的用户使用网络资源优先级。

2.5.2.1.1 应用优先级

应用报文优先级确定是指基于应用调整报文优先级，实现关键应用优先转发，比如视频会议、云桌面。应用优先级确定包含如下关键技术：

- 应用识别，是指在分析报文 IP 头的基础上，对报文的 4~7 层内容和协议字段进行提取和分析，识别报文所属应用名称。
- 多媒体智能调度，是指通过拥塞控制、QoS 差分服务等技术，精准抑制贪婪业务流量和优先调度音视频流量，保证高优先级业务服务质量的同时，提高带宽利用率。

2.5.2.1.2 用户优先级

用户优先级确定是指对关键用户优先提供网络服务。关键用户除了企业重要用户，还包括网络中的重要终端，比如会议室中的视频会议终端。优先接入、无线信号增强和无线优先转发等技术用于保障关键用户的无线网络体验。

1. 优先接入是指当接入用户数达到门限时，关键用户替换已接入的非关键用户正常接入，优先保障关键用户的接入体验。

- 2. 无线信号增强是指 AP 通过对关键用户所在位置的信号增强，解决关键用户在远离 AP 或移动场景下，信号差和不稳定的问题。
- 3. 无线优先转发是指通过 AP 为关键用户预留空口资源，在部分贪婪终端（非标抢占终端）开启大带宽业务（如大文件下载/上传、高清视频观看等）使得 AP 处于拥塞状态的情况下，提升关键用户的空口体验。

2.5.2.2 带宽确定

带宽确定是指不同业务在网络中传输需要占用的带宽可以相互隔离，数据传输过程中不会彼此干扰。在多业务承载的网络中，为避免多业务并发时带宽不足而导致关键业务丢包，可通过网络切片技术保障带宽。

网络切片技术是将物理网络中的资源划分给多个逻辑网络，每个逻辑网络服务于特定的业务类型或行业用户。每个网络切片都可以灵活定义自己的逻辑拓扑、SLA 需求、可靠性和安全等级，以满足不同业务、行业或用户的差异化需求。

2.5.2.3 时间确定

时间确定是指数据在端到端的传输过程中所需要的时间确定。传统网络除了必要的物理时延，还有队列发送、查表转发等造成的不确定时延。同时，传统网络尽力而为的通信机制从本质上缺乏确定性和实时性，无法满足工业制造等领域的时间确定要求。为了解决时延不确定问题，时间敏感网络（Time-Sensitive Networking, TSN）等技术应运而生。

TSN 在高精度时间同步的基础上，通过流规则识别出关键业务流量，对这些流量在精确时间点进行确定的调度，从而使得关键业务流量在经过设备单跳转发延时控制在微秒级别。其中关键技术包含高精度时间同步（如 IEEE 1588v2）以及流量调度机制（如 802.1Qbv 门控列表控制调度）等。

2.5.2.4 高可靠性

高可靠性考虑的是如何避免数据在转发过程中，因丢包、时延等造成的传输不可靠问题。随着时代发展，更多的业务（如付款业务、工业机器的 PLC 控制信息传输等）对于丢包变得愈发难以忍受，对网络可靠性要求越来越高。常见的降低网络丢包率技术如双发选收。

双发选收是指数据在网络入口设备进行复制，两份同样的数据经由不同路径送达出口设备，网络出口设备选择率先到达的一路数据进行转发。双发选收主要解决转发路径上的单点故障导致的报文丢失问题，显著地提升网络的可靠性。

2.5.3 关键指标

园区网络部署上述功能后，可以达到如下效果：

表 2-5 体验保障关键指标

分类	指标项	卓越	优秀
应用保障	链路拥塞场景，不降频不卡顿音视频分辨率	4K	720P
	协同办公场景，插入 10MB 图片耗时	6s	20s

分类	指标项	卓越	优秀
	云桌面时延	1080P 画质，时延 < 100ms	720P 画质，时延 < 1000ms
用户保障	时延	< 50ms	< 200ms
	带宽	带宽提升 30%	无法提升带宽
	故障告警功能	支持	不支持

2.6 绿色节能

2.6.1 绿色节能定义

园区网络绿色节能通常包括设备级节能、网络级节能和能耗可视等多个维度的实现。另外，园区智能化基础设施除了智能化管理，还可以利用无线局域网的感知能力来监测和识别环境变化，其感知能力与楼宇管理系统协同可以大幅优化空调和照明的能耗，减少园区能源浪费，以支持绿色建筑的目标达成。

2.6.2 绿色节能关键技术

2.6.2.1 设备级节能

设备级节能是指通过定义单设备不同负载下的节能模式的一种方法。例如空载时可以定义休眠模式/待机模式，低负载时可以定义低功耗模式等。

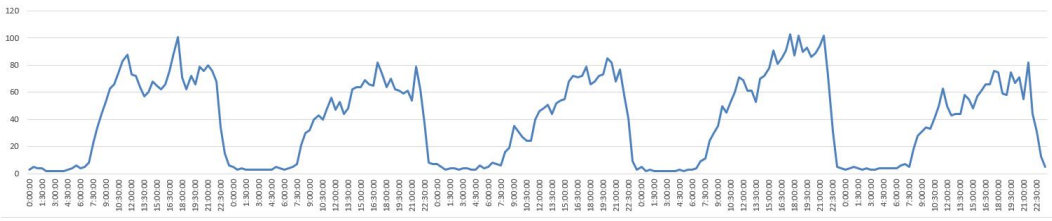
在 WLAN 系统中，AP 节点数量最多，因此 AP 的工作状态是节能方案的重点。因为 AP 部署通常通过 PoE 交换机供电，所以除了 AP 自身实现休眠、低功耗等方式，还可以实现 PoE 下电模式。

- **PoE 下电模式：**PoE 交换机端口停止对 AP 供电，AP 完全不消耗电力，启动 AP 时端口重新供电。
- **休眠模式：**仅用极低的功耗维持对 CPU 等关键硬件进行用电保护，其他器件进行关停。休眠模式下单 AP 可实现约 80%~90%的节能，恢复工作在一分钟以内。
- **低功耗模式：**相较于休眠模式，低功耗模式保持一定的通信能力。例如：将部分射频关闭。低功耗模式单 AP 可实现约 30%的节能，恢复工作在几秒到几十秒之间。

2.6.2.2 网络级节能

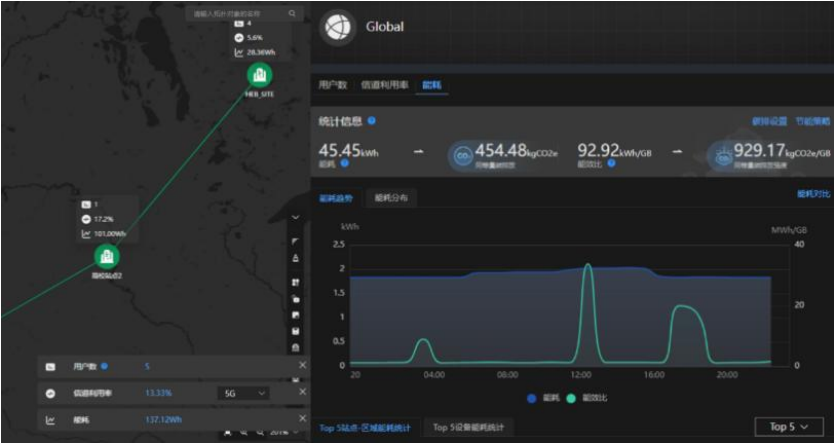
网络级节能是指通过分组定时关断、分区按角色关断是整网按时段、按设备角色关闭部分设备来实现网络级节能。利用 AI 分析网络潮汐特征和 AI 分区配置节能策略等，实现网络整体节能方案。如图展示了某学校教学楼 5 天的网络流量统计。可以看到的是，早晨 7 点网络使用量明显增长，在上午、下午达到使用高峰，凌晨 0 点后基本不使用。

图 2-14 某大学教学楼天网络流量统计图



网络能耗可视是指通过收集从 AP 等设备上报的能耗信息，可以实时监园区总网-楼宇-楼层-具体 AP 设备的能耗情况，并在智能分析系统上分析和展示。通常是网管系统或者 SDN 控制器的一部分，如图所示，系统可以展示区域级整网状态，包括但不限于区域级总体能耗按天/小时的信息统计、区域网络利用率（信道利用率）、区域级总体网络质量按天/小时的信息等。这种可视化管理可以帮助网络管理人员从整体上更直观地把握区域的能源使用状态，综合网络能耗和使用情况，进行合理地分时间分区域节能。

图 2-15 WLAN 网络可视化系统园区能耗监控



2.6.2.3 智能楼宇协同

智能楼宇协同是指 WLAN 网络与楼宇管理系统协同，实现空调、照明等楼宇设备节能的方案。楼宇能耗主要集中在空调和照明系统上，占总能耗的 75%以上。空调和照明主要为人服务，可采用类似“潮汐流量”的方式节能，晚上关闭照明，减少空调和照明能耗来节约能源。随着技术进步，WLAN 不仅能实现通信功能，且可通过 WLAN 的信道状态信息（Channel State Information）来感知空间和人员，可以为楼宇管理系统节能提供决策信息。

实施 WLAN 与智能楼宇管理系统协同节能，空调和照明系统的运行时间显著减少，与未实施节能策略前相比，空调能耗降低 15%~30%，照明能耗降低 15%~30%，为楼宇运营方节省了可观的电力成本，经济效益和环境效益显著。

2.6.3 关键指标

表 2-6 绿色低碳关键指标

分类	指标项	推荐值	基础达标值
设备节能	潮汐预测	AI 预测	人工预测
	无人时关断，轻载时休眠	支持	不支持
	唤醒时间	秒级	分钟级
	节能比	30%	网络节能 10%
感知节能	支持 CSI 感知有人无人，用于联动空调、照明等关断	支持	不支持

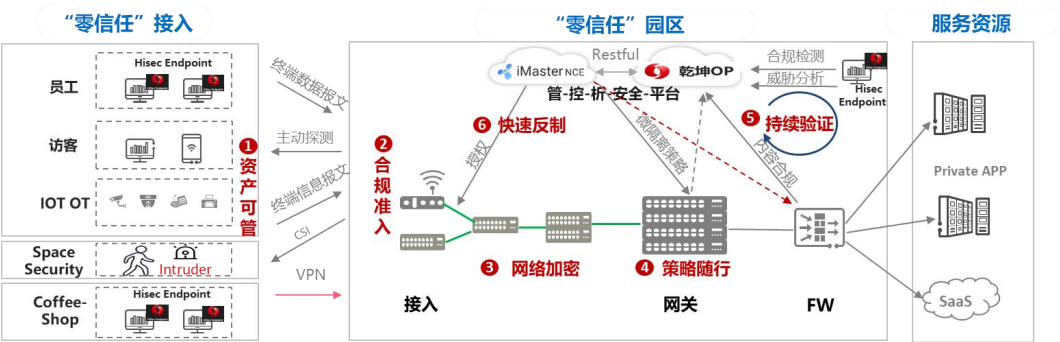
2.7 全域安全

2.7.1 全域安全定义

在园区场景下，全域安全旨在打造一个动态、智能的综合防护体系。它以统一策略平台为核心，整合各类安全能力，对园区全域（涵盖物理与虚拟资产、用户、业务流、数据及应用）实施闭环防护，切实保障业务连续性与数据安全。园区全域安全同样坚定基于“零信任”、“纵深防御”和“持续自适应”理念，通过技术的深度融合与协同联动，最终实现全空间（物理/虚拟）、全对象（资产/用户/数据）、全流程（访问/传输/处理）的无死角覆盖，是应对当下复杂网络威胁环境的关键解决方案。

零信任架构：安全防御的范式革命，基于零信任理念的园区安全解决方案从终端资产管理、终端合规接入、链路安全和微分段隔离，以及网安联动智能防御和韧性可信五个方面提供全方位安全防护。

图 2-16 园区网络安全架构



网络零信任安全：

-
1. 资产管理：终端识别可视，可根据终端指纹、信息识别终端类型，联动准入控制。
 2. 身份与访问管理：强化统一的身份治理、多因素认证和基于属性的动态访问控制。
 3. 链路安全：无线空口链路层防窃听，AP+交换机有线回传链路层安全防窃听（MACSec）。
 4. 微分段：在网络内部（尤其是东西向）实施细粒度的隔离策略，限制攻击横向移动的范围。
 5. 持续威胁检测：利用 AI/ML 技术，结合网络流量分析、端点检测响应和用户实体行为分析，实现对高级威胁的快速发现。
 6. 威胁风险响应：基于持续威胁检测精准识别风险来源，在网络接入近端实施自动响应，阻断风险端接入网络。

数据和供应安全及管理：

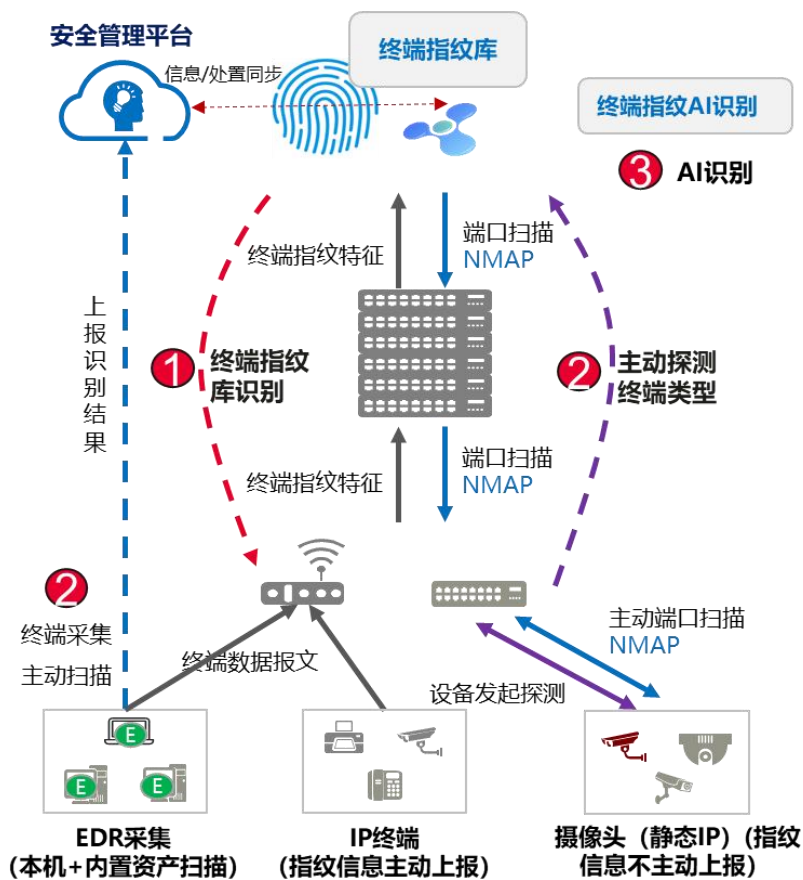
1. 数据安全治理：建立覆盖数据全生命周期的安全策略，包括数据分类分级、加密（传输中、存储中、使用中）、数据丢失防护、访问审计等。
2. 安全左移与 DevSecOps：在 IoT 设备固件开发、应用开发、云服务配置的早期就融入安全要求。
3. 统一的安全可视化管理：实现对分散、异构的终端、网络、云环境、数据的集中安全态势感知和策略管理。
4. 供应链安全：加强对 IoT 设备供应商、云服务提供商、软件供应商的安全评估和管理。

2.7.2 全域安全关键技术

2.7.2.1 资产管理

通过终端识别技术，建立清晰的终端台账信息，为园区内终端可视可观建立基础。终端识别是通过协议报文的摘要字段对终端特征进行分析提炼，识别出终端的类型、型号、厂商等信息。终端识别的方法主要包括被动指纹采集、主动扫描和人工智能聚类。包括被动流量识别、主动扫描、AI 智能识别等手段。

图 2-17 终端识别流程图



2.7.2.2 终端合规准入和微分段

应确保只有合法合规的终端才允许接入园区网络，并根据身份和合规状态分配不同网络权限。终端合规包括主机安全状态检查、安全接入认证（802.1X、Portal 等）、哑终端识别和防仿冒、终端防私接等。整合 RADIUS/TACACS+ 认证协议，实现用户入网、业务访问、运维操作的单点身份核验，杜绝越权风险。

网络安全微分段（Microsegmentation）是一种网络安全架构方法，其核心思想是将网络划分为细粒度的安全区域（或“微段”），并在这些微段之间实施严格的访问控制策略，以限制攻击者的横向移动（Lateral Movement），从而增强整体安全性。

图 2-18 微分段示例

安全组		基于安全组的策略控制矩阵				
组名	组ID		销售	研发	市场	...
销售	1	销售	√	×	√	...
研发	2	研发	×	√	√	...
市场	3	市场	√	√	√	...
...	...	...	...	...	...	...

2.7.2.3 链路安全

通过 WPA2/WPA3 等加密算法对空口进行加密，保证数据被抓取后需要解密后才能获取有效信息。在无线高安全场景下，通过空口加扰，实现非法用户无法抓取到有效的空口数据。有线链路通过 MACsec 实现物理层加密。

1. WPA

WPA（Wi-Fi Protected Access，Wi-Fi 保护访问）有 WPA、WPA2 和 WPA3 三个标准，是由 Wi-Fi 联盟制订与发布，用来保护无线网络访问安全的技术标准。支持 EAP-PEAP、EAP-TLS 等认证方式。

2. 空口信号加扰

空口信号加扰技术是通过多用户 MIMO（Multiple-input Multiple-output，多输入多输出）技术，利用 AP 多余的天线，发送额外的电磁波噪声，对终端的通信路径实现保护；在目标终端的位置范围内，因为干扰信号不影响真实数据，所以可以正确解调得出数据，在目标终端位置之外干扰信号影响真实数据，导致非法用户无法解调 Wi-Fi 信号，如下图所示，在目标终端位置之外，进行无线抓包侦听的时候，只能够抓到无效噪声。

图 2-19 空口加扰场景下不同用户收到的信号图



在终端移动场景下，空口加扰能在终端移动位置后，快速更新信息，保证空口加扰准确性。

3. MACsec

MACsec 是二层加密技术，提供逐跳设备的链路级数据安全传输。MACsec 的安全功能包含数据加密、完整校验、重放保护。MACsec 可适用于政府、金融等对数据机密性要求较高的场景。

2.7.2.4 网安智能防御

网安智能防御主要包括检测和响应，该方案的核心是通过数据统一、智能分析、策略协同和近源执行，构建自适应、精准化的主动防御体系，尤其适用于大型园区网络或云化环境。

图 2-20 网安智能防御分层

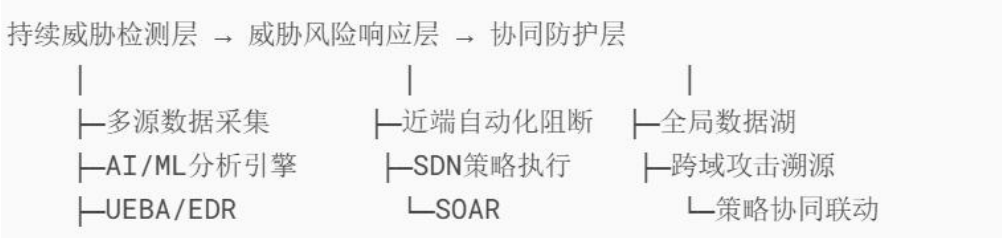


表 2-7 网安智能防御技术方向

技术方向	具体技术	作用
数据整合	安全数据湖（SIEM/SOC 平台）	统一存储与标准化多源日志
智能分析	AI 行为建模、图神经网络（GNN）	关联攻击链，精准溯源攻击者
策略执行	SDN、NFV（网络功能虚拟化）	动态编程网络设备，实现近源阻断
自动化编排	SOAR 平台 + API 集成	跨系统策略自动下发与响应
身份化控制	零信任架构（ZTNA）、基于标签的策略（如 SDP）	基于主体身份实施最小权限访问控制

2.7.2.5 韧性可信

韧性系统是网络设备的安全可信，指网络设备在保障安全性（机密性、完整性和可用性）的同时，也具备让用户信任其隐私保护、可靠性和稳定性的能力，从园区网络威胁看安全要求，需重点保护终端和服务上软件、数据、硬件等关键保护对象，能力覆盖管控平台、路由器、防火墙、交换机和 WLAN 等产品。

从全生命周期分析可以分解得到出厂可信、协议安全、运维可信、系统可信等关键能力要求：出厂可信、协议安全、威胁韧性防御网。

图 2-21 园区网络威胁示意图



2.7.3 关键指标

部署上述的终端、链路、设备安全功能后，网络可以达成如下所示安全能力：

表 2-8 零信任关键指标

分类	指标项	推荐值	基础达标值
无线安全	空口信号干扰	支持	不支持
无线安全	数据加密算法安全	WPA3	WPA2
有线安全	AP+交换机链路层安全加密：MACsec	无线+有线链路全链路支持，交换机支持国密	仅交换机支持，不支持国密
终端全可视	终端识别支持被动流量分析和主动扫描识别终端知产信息。	被动流量分析、主动扫描识别资产。支持 AI 聚类实现未知资产识别	被动流量分析、主动扫描识别资产
终端安全	基于零信任理念实现终端的安全合规准入	支持私接检测（交换机内置），支持 EDR 安全 Posture 检测	不支持私接检测或者旁挂设备支持，不支持 EDR 安全检测
微分段	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	不支持，或者仅支持 VxLAN 方式
网安联动	威胁支持通过网安协同实现威胁近源阻断	威胁支持联动交换机阻断	威胁支持联动安全设备阻断，不支持持续检测

分类	指标项	推荐值	基础达标值
主机安全	通过图引擎和人工智能技术加强未知高级威胁检测，及时发现高级远控、钓鱼、勒索、无文件攻击、0day，挖矿、窃密等异常行为。	支持安全通信、敏感数据安全保存、安全启动等设备安全能力	不支持

3

高品质万兆 AI 园区的典型应用

3.1 高品质万兆 AI 园区在教育

3.1.1 趋势与要求

全球教育体系正加速向数字化、智能化转型，以智慧技术重构教学、科研、服务与运营的全场景体验。

智慧教室的普及正在深刻改变传统教学模式，AI 驱动的个性化学习系统、AR/VR 沉浸式课堂等方式实现了教学过程的智能化、个性化和互动性，大幅提升了教学效果和学习体验。与此同时，在线教学和虚拟课堂的普及，打破了时空限制，让优质教育资源共享，缩小地区和个体间的差距，促进教育公平。这些现代化教学方式的有效运行，极大依赖于校园网络的高带宽、低延迟特性，网络的稳定性和实时性将直接影响教学的质量和体验。

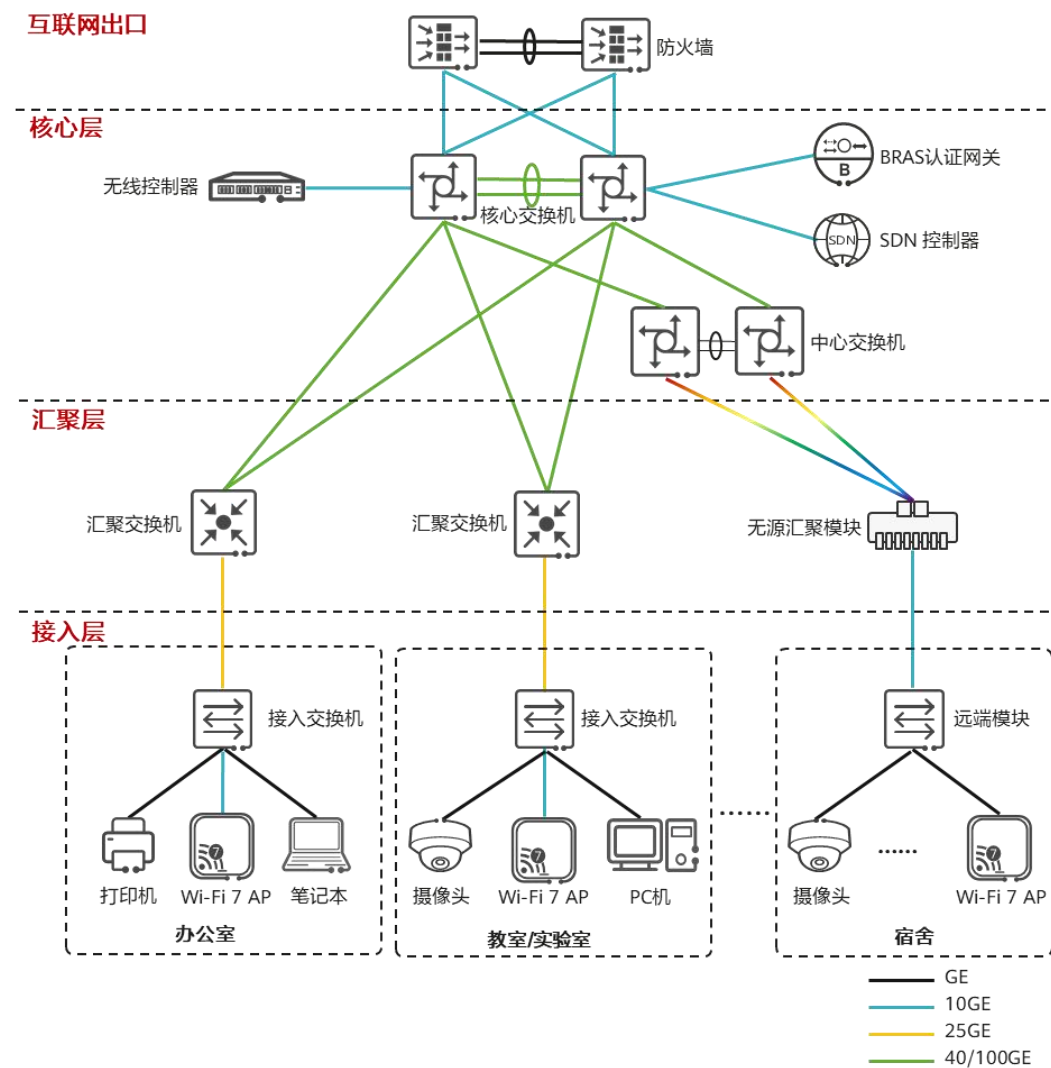
在科研活动中，人工智能技术在文献数据获取、实验预测、结果分析等方面发挥出重要作用。例如，在模拟复杂实验场景时，人工智能可提前预测实验结果，减少实际实验次数，提高科研效率。这就要求校园网拥有强大的算力支撑，满足人工智能模型训练、复杂数据运算的需求；网络传输速度要快，实现科研数据快速上传与下载，尤其在多团队协作共享数据时，保障数据交互高效进行；网络安全性更是重中之重，防止科研数据泄露，保护科研成果。

高校数字化转型不仅涉及教学和科研的变革，校园服务和运营管理的智能化也是智慧校园建设的重要组成部分。智慧校园通过构建一站式信息服务平台，整合教务、学工、图书、后勤等系统，为师生提供更加便捷、个性化的服务体验。物联网与智能技术正在革新校园基础设施管理和运营模式，加速运营从传统的人工操作走向自动化、智能化。大规模的移动设备和物联终端接入，对校园网络的覆盖、并发、可靠性都提出了新的要求。

3.1.2 推荐组网架构

典型的校园网包含办公室、教室、宿舍等场景，高品质万兆校园网络提供了万兆超宽、确定体验、智能运维和绿色低碳的网络，满足学校多元化业务和未来演进的需求。

图 3-1 推荐组网架构



3.1.3 智慧办公

越来越多的高校通过云办公平台（如 Microsoft 365、Google Workspace 等）来实现远程协作、在线文档编辑、任务跟踪、数据共享等功能，同时，疫情之后，Teams、Zoom 等线上会议爆发式增长，提升了教师在跨部门、跨校区协作的便利性，在提高工作效率的同时，也降低了运维成本。

云办公平台和高清视频会议，除了对网络带宽有诉求外，对网络时延也提出了更高的要求，如下表所示。

表 3-1 不同业务的网络时延要求

业务	带宽	时延
4K 高清视频/Streaming Ultra HD (4K) video	15~30 Mbps	20 ms

业务	带宽	时延
8K 高清视频/Streaming Ultra HD (8K) video	40~100 Mbps	20 ms
高清视频会议/HD video conferencing	5~7.2 Mbps	20 ms
实时文档协作	5~10 Mbps	<100 ms
云桌面	8~20 Mbps	≤50 ms
Sources: Huawei, Cisco, Microsoft, Frontier Communications, HealthIT.gov		

网络中的上传/下载等突发流量抢占了大量网络资源，可能会导致视频会议和协同办公出现卡顿等体验不佳的情况，同时由于视频会议和协同办公平台在云上部署，园区出口以外运营商网络的质量也是影响使用体验的关键因素。如何保障关键办公应用的体验，如何在出现问题时快速定位问题，是新形势下亟需解决的问题。

一张高品质万兆校园办公网络，建议指标如下表所示。

表 3-2 高品质万兆校园办公网络建议指标

项目	建议指标
入室部署的接入设备带宽	≥10Gbps
WLAN AP 标准	Wi-Fi 7
80MHz 组网，3 个 AP 下挂 18 终端总吞吐	≥960Mbps
4K 高清视频会议并发路数	≥60 路
视频会议、云桌面等关键应用清晰度和时延	1080P，时延<100ms
关键用户的业务时延	≤50 ms

3.1.4 智慧教室

现代教育正在经历前所未有的变革，传统课堂模式正在被智慧教室、在线教学、VR 沉浸式课堂等先进教学方式所取代。智慧教室通过整合多媒体设备、传感器和智能互动系统，为师生提供了一个更加动态、高效的学习环境。与此同时，在线教学和虚拟课堂的普及，使得高校教学突破了时间和空间的限制，学生可以通过网络在任何地方随时参与学习，这大大提高了教学的灵活性和可及性。

VR（虚拟现实）技术的引入更是为高校教学带来了前所未有的沉浸式体验。学生可以通过虚拟现实设备进入模拟实验室、远程操作高精尖的科研设备，甚至进行医学、工程等领域的仿真实验。这些现代化教学方式的有效运行，极大依赖于校园网络的高带宽、低延迟特性。网络的稳定性和实时性将直接影响教学的质量和体验，如果网络带宽不足或延时过高，将导致课堂互动的卡顿、虚拟场景加载延迟，影响整体教学效果。因此，万兆园区网络的部署将为智慧校园中的新型教学模式提供高速、稳定的网络支持，确保教师和学生之间的信息传输流畅，教学过程更加高效、互动性更强。

表 3-3 业务对带宽和时延的要求

业务	带宽	时延
在线课堂/Online class	10~20 Mbps	< 100 ms
标准 AR 及 VR（娱乐）/ Standard AR&VR (entertainment)	≥30 Mbps	≤20 ms
增强 AR 及 VR（培训）/Advanced AR&VR (training)	>80 Mbps	15 ms

学校是一个大型的能源消耗场所。众多的教室、实验室等空间，每天都在消耗大量的电能。尤其是网络设备、空调和灯光，往往在无人使用的情况下仍然持续运行，造成了极大的能源浪费，也给学校带来了高额的运营成本。传统的能源管理方式需要人工巡查各个教室，不仅耗时耗力，而且容易出现疏漏。为了建设绿色校园，降低运营成本，学校迫切需要一套智能节能系统。

一张高品质万兆校园教室网络，建议指标如下表所示。

表 3-4 高品质万兆校园教室网络建议指标

项目	建议指标
入室部署的接入设备带宽	≥10Gbps
WLAN AP 标准	Wi-Fi 7
80MHz 组网，3 个 AP 下挂 18 终端总吞吐	≥960Mbps
在线课堂应用清晰度和时延	1080P，时延< 100ms
免传感器，WLAN AP 通感一体，感知人员存在，联动楼宇管理系统进行照明、空调等节能	支持
彩光端口密度	≥96 个/设备

3.1.5 智慧宿舍

随着高校教育和学生生活需求的不断变化，大学宿舍的业务需求也呈现出多样化和智能化的发展趋势。现代大学宿舍不仅仅是提供住宿的场所，更成为学生学习、娱乐和社交的综合空间。宿舍内需要满足高速的互联网接入，以支持学生进行在线学习、远程课堂、视频会议等教学活动，同时也需要稳定的网络环境来支持流媒体观看、游戏娱乐和社交应用的使用。

因此，高校宿舍对网络的要求日益增高。首先，宿舍需要具备高带宽、低时延的网络基础设施，以保障多个设备同时在线时的流畅体验。其次，随着物联网技术的发展，智能宿舍逐渐成为趋势，学生的门禁、照明、空调、温控等设施都需要通过网络进行智能化管理，这对网络的可靠性和稳定性提出了更高的要求。此外，传统的手动运维

模式已难以满足大规模、高并发的网络需求，学校需要采用更为智能和自动化的运维解决方案。

一张高品质万兆校园教室网络，建议指标如下表所示。

表 3-5 高品质万兆校园宿舍网络建议指标

项目	建议指标
入室部署的接入设备带宽	≥2.5Gbps
WLAN AP 标准	Wi-Fi 7
8 个终端并发接入时单终端带宽	≥50bps
在线课堂、实时游戏时延	< 100ms
免传感器，WLAN AP 通感一体，感知人员存在，联动楼宇管理系统进行照明、空调等节能	支持
覆盖类、干扰类、高信道利用类、空口拥塞类和漫游类 Wi-Fi 问题，无需人工干预，系统自动优化和闭环	支持
自然语言交互，问题分钟级定位	支持

3.2 高品质万兆 AI 园区在政府

3.2.1 趋势与要求

根据《2024 联合国电子政务调查报告》显示，全球已有 81%的国家发布了数字政府策略，探索如何构建新型数字化政府，实现政府决策科学化、行政办公高效化、公共服务便捷化和社会治理精准化。

全球各地政府加速建设一体化政务服务平台，编织政务“一张网”，实现跨地区、跨部门、跨层级业务协同，提供“一站式”高效政务服务，让政务服务真正实现普惠化。根据《2022 联合国电子政务调查报告》，全球 138 个国家在线提供多种政务服务，其中 115 个国家提供跨部门、跨层级整合的政务服务。政务网络需要广泛覆盖将服务送到群众中去，也需要打破部门壁垒让数据跨部门、跨层级、跨区域畅通共享，才能真正提供普惠化的“一站式”政务服。

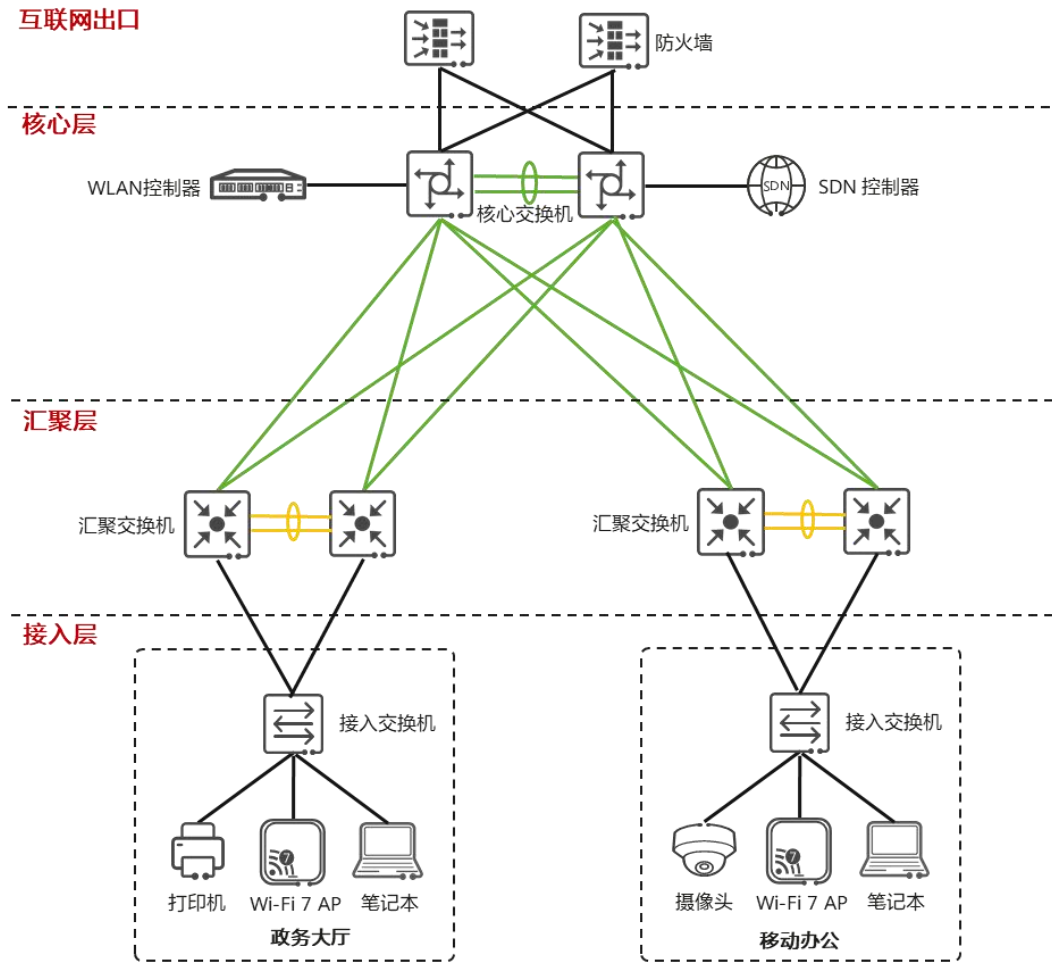
全球政府移动应用访问量年均增长超过 30%，疫情之后，视频会议在政令上传下达、跨部门协同中的使用频率增长了 3-5 倍。提升移动化接入品质、视频保障能力和运营运维效率，打造政务随身办、会议随时连的高效办公体系和视频会议体系，提升党政办文、办公、办会效率，是政府高效运行的必要支撑。

随着政务移动化以及业务系统复杂度提升，安全风险也随之增加。同时，新兴网络攻击技术手段层出不穷、日新月异，国家关键信息基础设施面临的网络安全形势日益严峻。根据白宫《美国政府网络安全年报》，美国各政府部门平均每年发生 3.2 万起网络安全事件。由此可见，构建终端接入、网络传输、空间、隐私等一体协同的安全体系是数字政府建设的重要保障。

3.2.2 推荐组网架构

典型的政府园区网包含政务大厅和移动办公等场景，高品质万兆政府园区网络提供了万兆超宽、全域安全和体验保障的网络，满足政府数字化转型需求。

图 3-2 推荐组网架构



3.2.3 政务大厅

作为政府与公众互动的重要窗口，政务服务大厅正加速向“线上线下一体化”转型，推动“一网通办”和“跨地域通办”，实现数据共享与智能服务。业务办理逐步向线上迁移，大厅功能转向复杂业务办理、咨询及特殊群体服务。同时，智能化带来服务升级，AI 智能客服、AI 材料预审，AI 导办机器人快速普及，减少人工窗口压力；VR/AR 虚拟大厅导航、远程视频帮办等应用助力提升用户体验。

政务大厅的智能化升级，对网络基础设施也提出了新的需求。首先，满足群众和工作人员随时随地移动办理业务的诉求，需要广泛覆盖、无死角的极速 Wi-Fi 网络。其次，智能客服、智能导办等智能化应用需要实时响应，减少群众等待时间，这就要求网络具备高带宽，能承载大流量数据传输，并且延迟低，保证业务办理流畅，系统响应迅速。另外，政务服务涉及大量个人隐私和企业机密信息，网络必须具备强大的安全防护能力。

一张高品质万兆政务大厅网络，建议指标如下表所示。

表 3-6 高品质万兆政务大厅网络建议指标

项目	建议指标
入室部署的接入设备带宽	≥10Gbps
WLAN AP 标准	Wi-Fi 7
大厅内随意移动，业务不中断	支持
Wi-Fi 防窃听	WPA3 + 物理噪声干扰防护

3.2.4 移动办公

随着数字化转型加速，全球政府机构正全面推进无线化办公，以提升行政效率、增强灵活性和优化公共服务。政府工作人员广泛使用笔记本电脑、平板电脑和智能手机等移动设备处理公务，实现随时随地的办公需求。Wi-Fi 网络在带来便利的同时，也提升了信息泄露的风险。全球范围内的 Wi-Fi 漏洞（如 2017 年的 Wi-Fi WPA2 密钥重装攻击和 2021 年的 FragAttacks 等）以及区域不断爆发的 Wi-Fi 网络攻击，加剧了政府客户对 Wi-Fi 安全的担忧；部分政府部门仅在少量区域部署 Wi-Fi，阻碍了无线化进程。

全球政府视频会议应用呈现爆发式增长，数据显示，2023 年全球 92% 的国家级政府机构已部署云视频会议系统，会议频次同比 2020 年增长 340%。预计到 2026 年，政府视频会议市场规模将突破 80 亿美元，年均复合增长率维持 18%以上。持续增长的视频会议应用，对网络带宽、低延迟和安全防护提出更高要求。

一张高品质万兆政务办公网络，建议指标如下表所示。

表 3-7 高品质万兆政务移动办公网络建议指标

项目	建议指标
入室部署的接入设备带宽	≥10Gbps
WLAN AP 标准	Wi-Fi 7
Wi-Fi 接入，用户在办公区内移动，业务不中断且无感知	支持
4K 高清视频会议并发路数	≥60 路
Wi-Fi 防窃听	WPA3 + 物理噪声干扰防护
终端防私接和防仿冒	支持

3.3 高品质万兆 AI 园区在金融

3.3.1 趋势与要求

金融机构的数字化转型在经历了以物理网点进行服务的 Bank 1.0 时代、提供自助服务如 ATM 机的 Bank 2.0 时代、通过 APP 等移动入口随时随地提供服务的 Bank 3.0 时代、金融科技重构银行业务的 Bank 4.0 时代之后，AI 正在驱动银行业务迈入 Bank 5.0 时代。

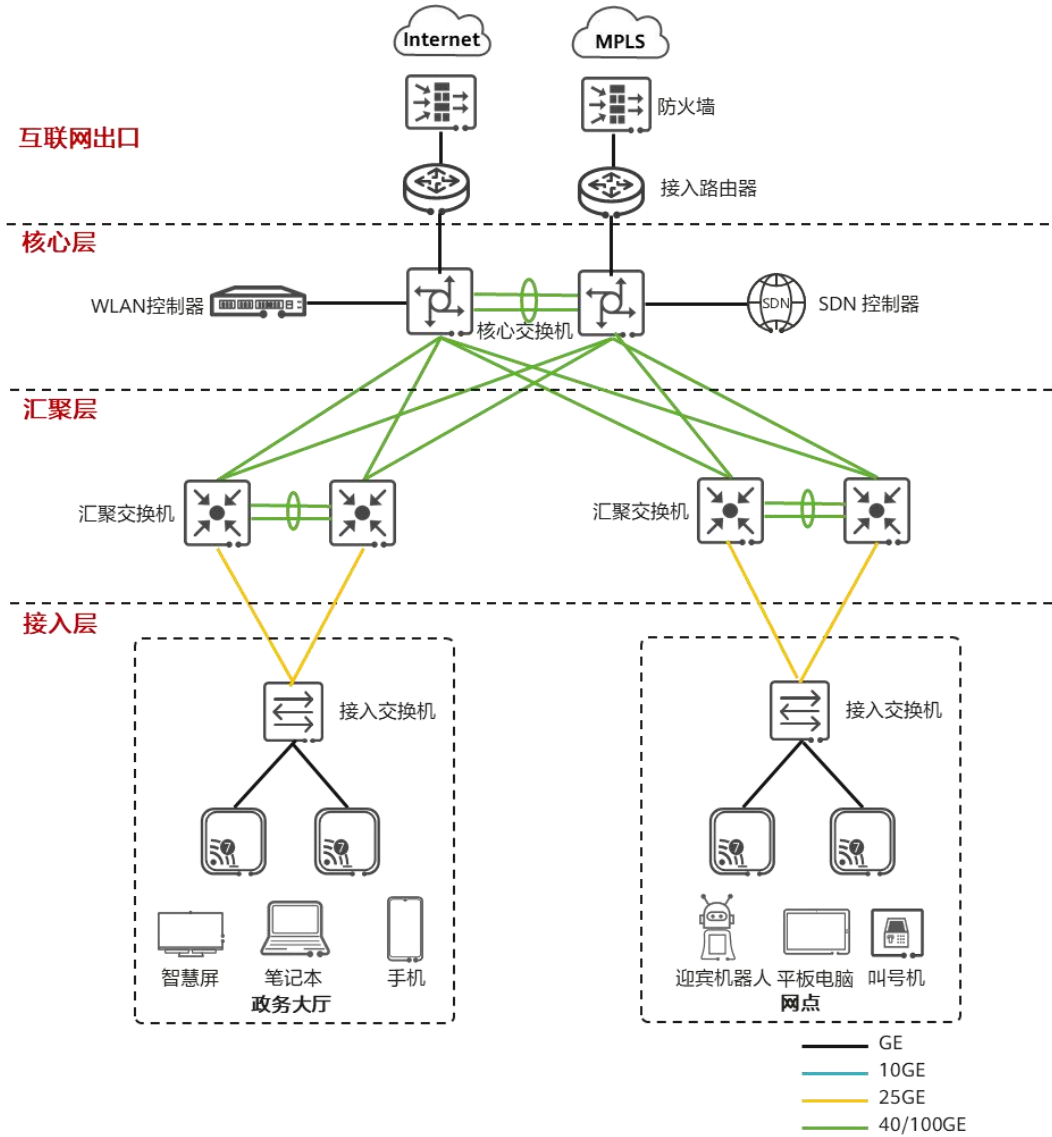
在 Bank 5.0 时代，银行正加速向智能化、以客户为中心的全面升级，实现沟通高效化、运营智能化和体验场景化。在高效沟通方面，银行广泛部署视频会议、智能客服和企业协同平台，实现总部与分支机构间的实时沟通与高效决策；在智能运营方面，通过 AI、大数据和流程自动化，提升风控、运营调度与 IT 系统管理的智能化水平，降低运营成本、增强敏捷性；在体验场景化方面，智能终端、远程柜员、无感排队与线上线下一体化服务正成为标配，为客户带来更便捷、高效、个性化的服务体验。

Bank 5.0 对银行的网络基础提出更高要求——需保障业务系统的稳定运行、海量终端的高密接入、远程视频与数据流的低时延传输，以及安全隔离与智能运维能力，构建敏捷、安全、可持续演进的数字底座。

3.3.2 推荐组网架构

典型的金融园区网包含智慧办公和智慧网点场景，高品质万兆金融园区网络提供了万兆超宽、全域安全和确定体验的网络，满足 Bank 5.0 演进需求。

图 3-3 推荐组网架构



3.3.3 智慧办公

随着疫情后混合办公模式的常态化，以及全球化运营的推进，视频会议成为金融行业跨区域沟通的核心工具。根据 Gartner 预测，未来 3 年视频会议将以 15%-20% 的 CAGR 增长。同时，员工随时随地访问工作环境的灵活性，以及银行业对数据安全和合规的高要求，也催生了云桌面在银行的快速普及。另一方面，随着银行业务的多样化和跨部门协作需求的增加，Microsoft 365 等协同办公应用成为了提升效率、优化流程和推动数字化转型的重要工具。

视频会议、云桌面和协同办公等核心工具的体验，直接影响了员工的工作效率。金融行业迫切需要一张能够保障关键应用确定性体验的高品质网络。

一张高品质智慧办公网络，建议指标如下表所示。

表 3-8 高品质万兆金融智慧办公网络建议指标

项目	建议指标
入室部署的接入设备带宽	≥10Gbps
WLAN AP 标准	Wi-Fi 7
80MHz 组网，3 个 AP 下挂 18 终端总吞吐	≥960Mbps
4K 高清视频会议并发路数	≥60 路
视频会议、云桌面等关键应用清晰度和时延	1080P，时延<100ms
关键用户的业务时延	≤50 ms

3.3.4 智慧网点

银行网点正加速从传统服务窗口向智能化、数字化、自助化的综合服务平台演进。智能客服、智能柜员机（VTM）、智能迎宾机器人的引入，提供了高效自助服务接口，减少客户等待时间。虚拟理财顾问、元宇宙银行体验区、AR 产品展示等新形式，增强了互动性，提升了客户体验和运营效率。业务升级需要一张依赖高并发、高安全、集中管理，以及智能保障高优先级应用的高品质网络。

一张高品质智慧网点网络，建议指标如下表所示。

表 3-9 高品质万兆金融智慧网点网络建议指标

项目	建议指标
WLAN AP 标准	Wi-Fi 7
智能终端在网点移动，业务不中断	支持
4K 高清视频会议并发路数	≥60 路
视频会议、云桌面等关键应用清晰度和时延	1080P，时延<100ms
关键用户的业务时延	≤50 ms
Wi-Fi 防窃听	WPA3 + 物理噪声干扰防护
终端防私接和防仿冒	支持

3.4 高品质万兆 AI 园区在医疗

3.4.1 趋势与要求

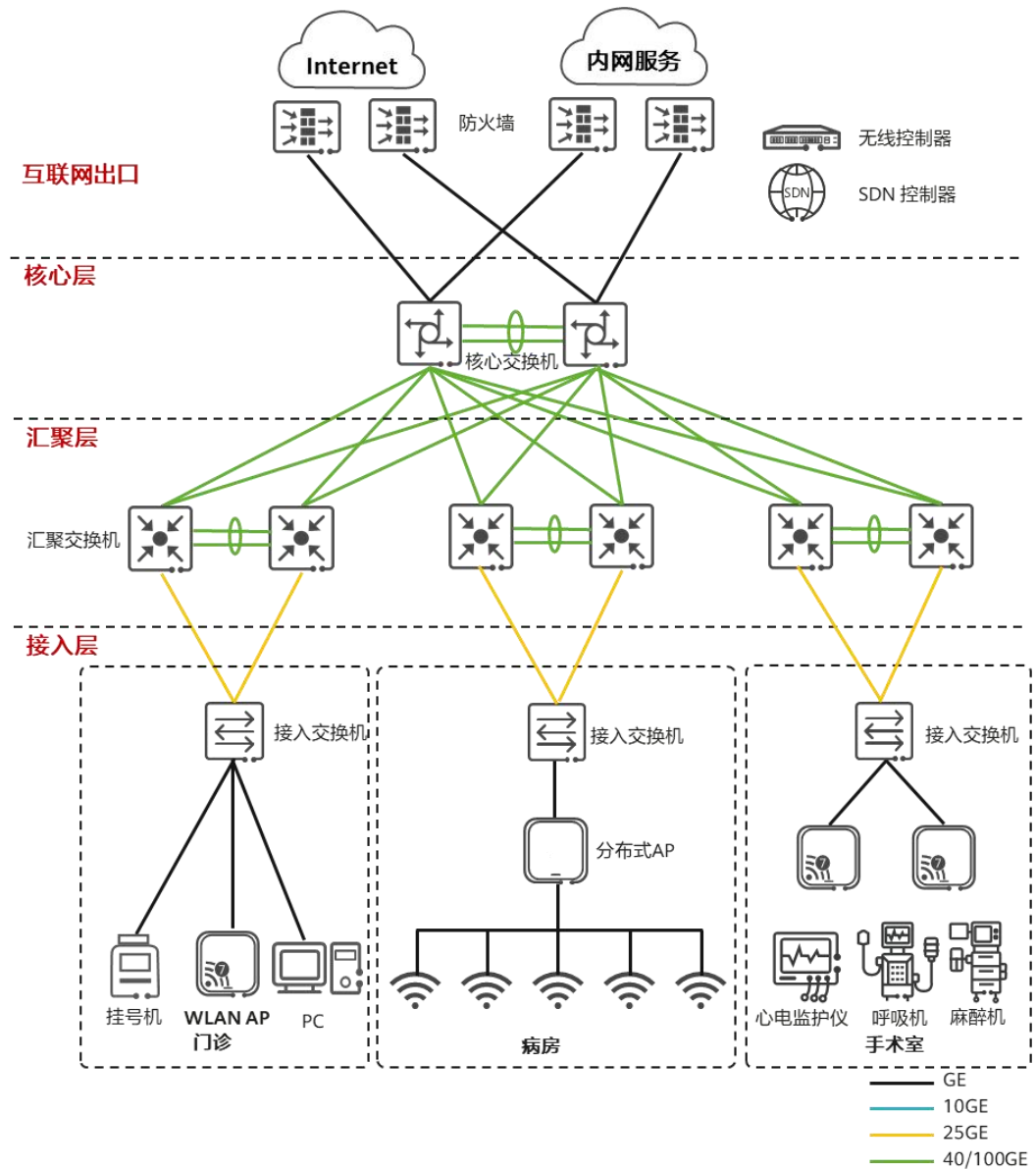
当前医院正处于全集成化迈入智慧化的过渡期，过去建设的烟囱式应用、割裂的数据孤岛无法与医疗业务很好的匹配协同，如何实现全院数据互联互通以及数据共享，发挥医疗数据在临床诊疗中的最大价值，一直是医院亟待解决的问题。通过智慧医院建设，实现全院数据一体化、严格的数据安全控制、符合国际医疗标准的医疗数据调用和智能预警系统，最终实现患者医疗数据的整体性、有效性和安全性，有效地优化医院资源，提高医院的整体运作效率和竞争能力。

2022 年中国医院普通门急诊就诊人次超 17 亿，住院人次超 1.6 亿，手术台次超 8000 万。面对巨大的医疗服务需求，提升门诊服务质量、病区管理效率和重症手术水平是保障医疗服务质量，加速医院智慧化建设的重要手段。

3.4.2 推荐组网架构

典型的医疗园区网包含门诊、病房和手术室等场景，高品质万兆医疗园区网络提供了万兆超宽、全域安全、泛在连接的网络，满足智慧医疗建设需求。

图 3-4 推荐组网架构



3.4.3 智慧门诊

门诊是医院服务的窗口，是患者到医院的第一站，门诊服务的优劣直接影响医院的形象。2022 年，中国门急诊就诊超 17 亿人次，但全国医生和护士数量不到 1000 万，极低的医患比使得门诊就医：挂号时间长、缴费时间长、等待时间长，看医时间短的“三长一短”的问题长期存在，看病时间往往不到 10 分钟，非看病时间则长达 40~80 分钟。

一张高品质智慧门诊网络，建议指标如下表所示。

表 3-10 高品质万兆智慧门诊网络建议指标

项目	建议指标
----	------

项目	建议指标
入室部署的接入设备带宽	≥10Gbps
WLAN AP 标准	Wi-Fi 7
终端 Wi-Fi 接入，在门诊移动，业务不中断	支持
GB 级医学影像调阅速度	秒级
30 用户 Wi-Fi 并发接入总吞吐	≥340Mbps

3.4.4 智慧病房

经过门诊医生问诊和检查，如果患者需要进一步治疗，就需要住院了。2022 年，中国 500 张床位以上医院 人床比为 1.6~1.7，而美国梅奥诊所人床比为 28.2，二者相差接近二十倍。极低的人床比导致医护人员工作繁重，50%的医护人员每月加班时长在 60 小时以上。

病区移动查房目前主要使用无线 PDA 设备，完成患者病历查看，记录患者诊疗数据以及下达医嘱，但是由于医生查房时需要在不同病房穿梭，PDA 跨 AP 漫游可能会发生丢包，从而导致 PDA 反复登陆，严重影响医生查房效率。

一张高品质智慧病房网络，建议指标如下表所示。

表 3-11 高品质万兆智慧门诊网络建议指标

项目	建议指标
移动查房时 PDA 业务零中断	支持
入室部署的接入设备带宽	≥2.5Gbps
WLAN AP 标准	Wi-Fi 7
内网、外网、物联网三网合一	支持
心跳频率、呼吸频率、病人摔倒无感监测	支持

3.4.5 智慧手术室

ICU 病房为各类危重症患者提供系统、高质量的医学监护和救治，是医院集中监护和救治重症患者的专业科室，是危重症患者最后的“守护神”。ICU 病房汇聚了几十种床旁设备，除监护仪、呼吸机、输液泵、微量注射泵等基础设备外，根据情况还会配备除颤仪、心电图机、心脏起搏器、血气生化分析仪等设备。手术室里麻醉医生也是守护患者的最关键角色之一，他需要在手术过程中时刻关注各种医疗设备上显示的患者生命体征，及时进行干预。

越来越多的先进设备应用于 ICU 和手术室，极大提高了救治的时效性和成功率，但是由于设备种类多、厂商多、标准千差万别，导致各种设备独立工作，不具备互操作

性，ICU 病房和手术室产生的大量的临床数据需要医护人员手工记录和研判，不但给医护人员造成很大负担，而且由于手工记录数据的不连续、非标准化等问题，导致临床数据无法发挥最大价值。

一张高品质智慧手术室网络，建议指标如下表所示。

表 3-12 高品质万兆智慧手术室网络建议指标

项目	建议指标
入室部署的接入设备带宽	≥10Gbps
WLAN AP 标准	Wi-Fi 7
内网、外网、物联网三网合一	支持
核心交换机升级业务不中断	支持

3.5 高品质万兆 AI 园区在制造

3.5.1 趋势与要求

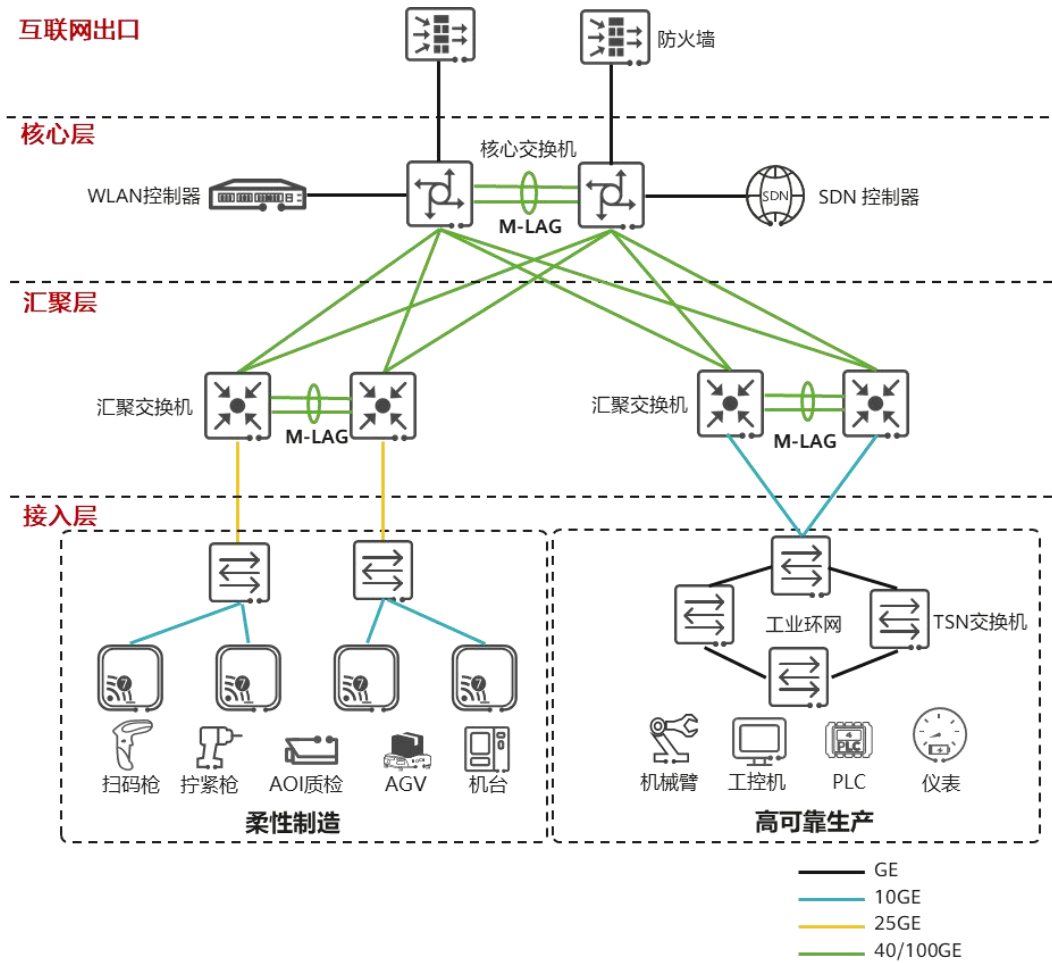
智能制造正朝着高度数字化、智能化和柔性化方向发展。随着工业物联网（IIoT）、人工智能（AI）、5G、边缘计算等技术的融合应用，制造企业逐步实现设备互联、数据驱动、流程协同和自主决策，向“预测性维护”“柔性产线”“个性化定制”和“绿色低碳”演进。未来，智能制造将以数字孪生和工业大模型为核心，推动产业链智能协同和全生命周期优化，助力制造业向高质量、可持续方向转型升级。

在向智能制造的演进过程中，网络是基础底座，联接人-机-料-法-环等生产要素，支撑着数据的产生、采集、流转、处理和价值变现。构建网络底座一方面需要将各类生产要素联网，另一方面要满足生产要素及上层应用对联接的需求。围绕制造企业的价值链，推动研发、生产、运营等各业务领域向智能制造转型升级，网络需要支撑和保障稳定生产、柔性制造、加速研发和安全运营。

3.5.2 推荐组网架构

典型的制造网络实现了 IT 和 OT 的融合，打通了“数据孤岛”，将 MES、ERP、SCADA、PLC 等系统集成到统一网络中，可实现实时数据采集、分析和反馈，支持预测性维护、产线优化、柔性生产等应用，赋能业务实时协同、精准决策和持续创新，构筑起智能制造的基础。

图 3-5 推荐组网架构



3.5.3 高可靠融合生产网

制造企业的每个生产单元都有自己的产能指标及生产节拍，比如上汽宁德工厂就是60JPH（Jobs Per Hour）的生产节拍，即一分钟一台车。近期，日本某知名汽车制造商的14家工厂因为IT系统故障造成停产1.5天，直接影响14000台汽车的生产交付。稳定量产就是确保生产过程的稳定性、连续性，按计划执行生产，从而避免可能的经济损失。实现稳定量产，需要围绕人、机、料、法、环等各方面进行可靠性管理，比如生产中的原材料、能源表计、生产装备等。网络作为数据联接底座，联接生产管理和生产执行系统（ERP、MES、SCADA、PLC、I/O等），需要通过全时在线的高可靠连接，以保证企业生产的连续性。

定制化、多元化产品逐渐成为制造业的普遍需求，同时企业内部出于缩短交付时间、节约生产成本、提升设备利用率的考虑也在积极推进柔性制造。市场研究数据显示，全球未来5年柔性制造的市场规模年符合增长率达20%。制造企业的订单不同，其生产工序也要随之调整。因此，产线调整效率、生产装备甚至整个车间自身的柔性化能力成为企业关注的重点。这就要求企业通过自动化、机器人、智慧物流等技术，构筑起柔性制造系统。网络也需要适配产线调整的场景要求，灵活接入相关终端设备。传统的有线网络接入方式涉及到接入点位规划、布线施工等，很难满足柔性制造的需求，采用无线网络使得生产装备“剪辫子”，已逐渐在制造企业规模应用。

一张高可靠融合生产网络，建议指标如下表所示。

表 3-13 高可靠融合生产网络建议指标

项目	建议指标
WLAN AP 标准	Wi-Fi 7
单用户 Wi-Fi 极限速率	≥3.5Gbps
Wi-Fi 漫游丢包率	≤0.1%
链路故障切换时间	≤50ms，业务不中断
工业环网故障切换时间	≤20ms
控制业务丢包率	0%
1588v2 时钟精度@64 跳	1us
视频会议、云桌面等关键应用清晰度和时延	1080P，时延<100ms
关键用户的业务时延	≤50 ms
IT/OT 网络统一运维	支持

3.6 高品质万兆 AI 园区在零售

3.6.1 趋势与要求

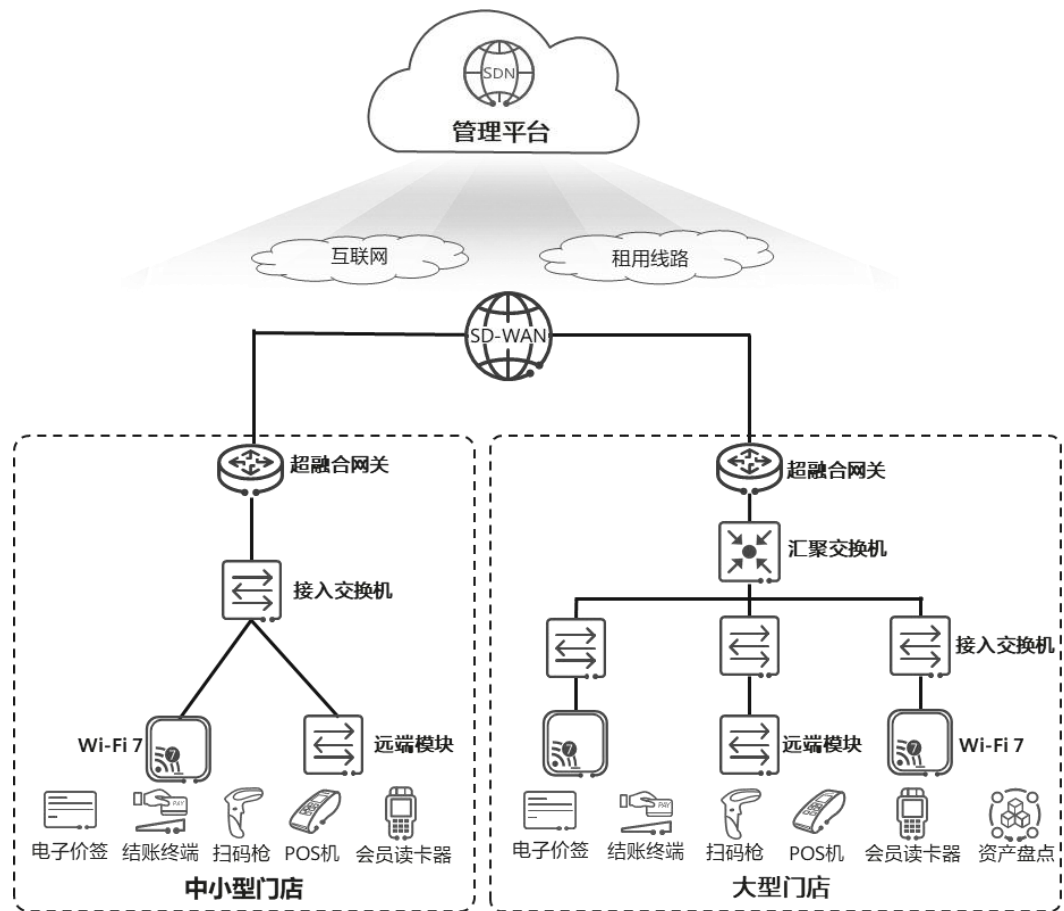
零售行业正在进行数字化转型与全渠道零售的加速融合，零售商正通过电商平台、线下门店、移动应用、社交媒体和智能设备等多个渠道连接消费者，提供无缝购物体验。特别是在人工智能、物联网、云计算和大数据分析等技术的驱动下，个性化推荐、自动化仓储与配送、以及智能客服等技术正在逐步提升顾客体验和运营效率，加速零售行业走向智慧化。

随着消费者对个性化、便捷化、即时化购物体验需求的不断增长，零售商持续投入智慧门店的建设。智慧门店作为零售数字化转型的核心载体，通过 IoT、AI、AR/VR、智能导购等技术的创新和应用，实现“人、货、场”的智能化升级，提供更便捷和更高效的购物体验。

3.6.2 推荐组网架构

典型的智慧门店网络通过集成物联网、人工智能、大数据分析和自动化技术，实现"人、货、场"全要素实时智能互联，为顾客提供个性化、无缝化、便捷的购物体验，同时实现高效、智能的运营管理。

图 3-6 推荐组网架构



3.6.3 智慧零售门店

传统门店采用纸质标签标注商品价格，效率低、易出错且灵活性差，越来越多的门店开始选择电子价签。电子价签能自动同步价格、促销信息及库存状况，避免人工更换价签的误差和延迟。同时，电子价签提供清晰的显示和动态内容，增强了顾客的购物便利性与互动体验，并且符合环保趋势，降低纸张浪费，为零售商提供了更灵活、精准的运营和营销方式。

基于市场竞争和消费需求的快速变化，零售商需要通过标准化、自动化、数字化和灵活的运营支持，确保在短时间内完成门店的业务敏捷上线；同时通过集中式的管理，实现门店网络多维可视，故障快速定位，从而降低运营成本，提升运营效率。

一张典型的高品质智慧门店网络，建议指标如下表所示。

表 3-14 高品质智慧门店网络建议指标

项目	建议指标
WLAN AP 标准	Wi-Fi 7
电子价签部署	PCIe 插卡/内置协议方式融合在 WLAN AP

项目	建议指标
业务开通	自然语言交互的意图开局，模板化开局
运维管理	多门店统一管理，应用/终端/网络三维可
出口网关	超融合网关，融合 5G、WAC、路由、安全、交换等功能

3.7 高品质万兆 AI 园区在酒店

3.7.1 趋势与要求

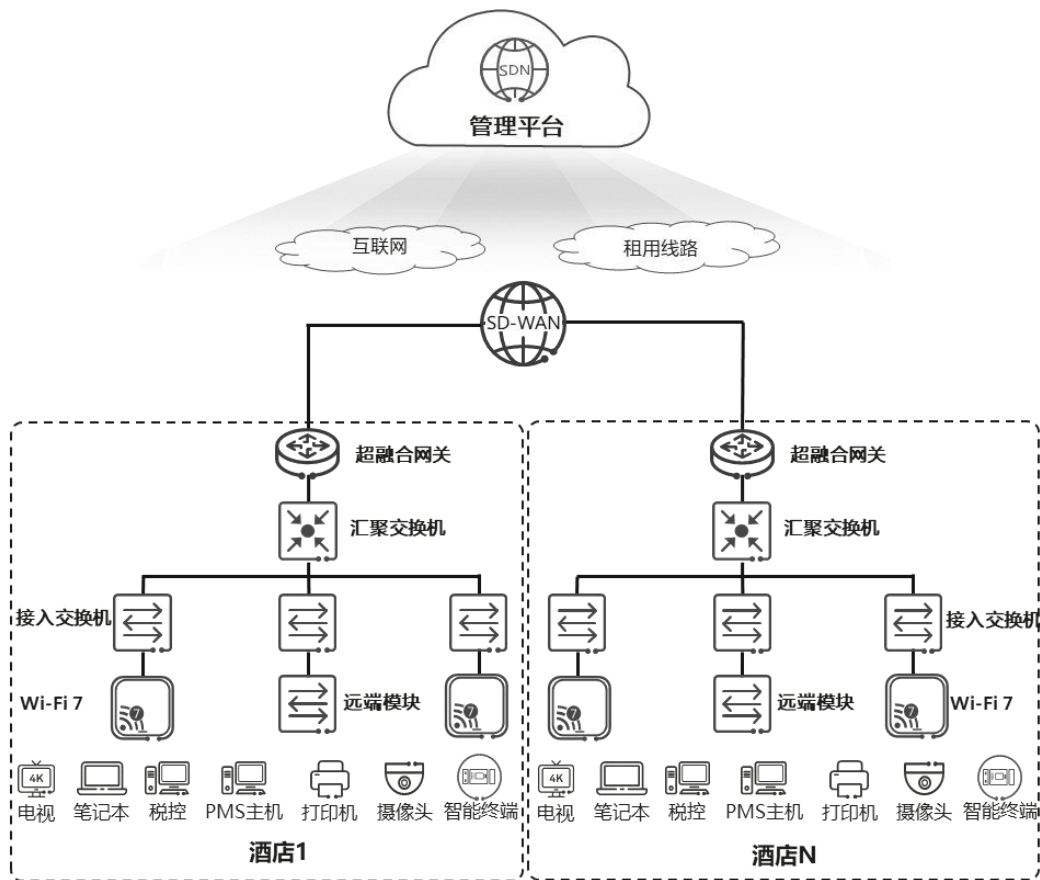
酒店行业正经历数字化、个性化和可持续发展转型。随着顾客对个性化服务的需求不断增加，酒店通过智能化设备、移动应用、AI 驱动的个性化推荐、虚拟助理等技术提升客人体验。同时，环保和可持续发展成为行业的重点，绿色酒店和节能建筑逐渐成为标准。

网络基础设施是酒店数字化转型的基石，它不仅支持所有智能设备和应用的稳定运行，还能提高运营效率、提升顾客体验、增强安全性、支持数据分析与营销等多方面需求。随着技术的不断进步和顾客需求的变化，酒店网络基础设施的可靠性、扩展性和安全性将决定其在未来市场中的竞争力。

3.7.2 推荐组网架构

典型的酒店网络网络通过 IoT 融合、人工智能等技术，在满足高速和稳定的基本需求，还提供了安全、灵活、自动化和可扩展的解决方案，确保顾客在各类设备和服务中享受流畅、个性化的体验，以支持现代酒店的数字化转型，提升运营效率和顾客满意度。

图 3-7 推荐组网架构



3.7.3 智慧酒店

智慧酒店需要一张高性能、全覆盖、智能化的无线网络，能够在客房、公共区域、会议室、餐厅等所有区域提供稳定且高速的无线连接。网络必须具备高带宽和低延迟，能够承载智能设备、物联网（IoT）应用、视频流、移动支付和智能控制系统等多个高流量应用，同时支持高并发连接，确保在高峰时段也能流畅运行，提升顾客体验并优化运营效率。

全球范围内的酒店连锁化带来酒店新建机会，为了迅速响应市场变化、降低开店时间和成本、以及提升运营灵活性，酒店希望能够在较短的时间内完成新酒店的开设与运营，以适应市场快速变化和激烈竞争。

酒店对于绿色节能的需求日益增长，逐渐采用节能建筑设计、可再生能源（如太阳能和风能）、网络动态节能、智能照明/空调系统优化、以及高效水资源管理等技术，以降低能源消耗和运营成本。

一张高品质智慧酒店网络，建议指标如下表所示。

表 3-15 高品质智慧酒店建议指标

项目	建议指标
WLAN AP 标准	Wi-Fi 7

项目	建议指标
单用户 Wi-Fi 极限速率	$\geq 3.5\text{Gbps}$
Wi-Fi 漫游丢包率	$\leq 0.1\%$
绿色节能	AP 动态节能，CSI 感知节能
业务开通	自然语言交互的意图开局，模板化开局
运维管理	多门店统一管理，应用/终端/网络三维可视

4 产业展望

4.1 产业展望

在数字化转型的浪潮中，园区网络作为各类场景数字化建设的基石，正经历着深刻变革。Wi-Fi 技术的代际演进持续为网络翻新注入强大动力，与此同时，AI+安全+物联融合的趋势也在全方位推动园区网络的整体更新与升级，构建更加智能、高效、安全的网络环境。

在 Wi-Fi 技术的代际演进方面，未来 5 年，Wi-Fi 8 的问世将会进一步加速网络升级，Wi-Fi 6 向 Wi-Fi 7 升级将会必然趋势，部分园区将率先体验 Wi-Fi 8 带来的极致网络；随着 Wi-Fi 的升级、8K 摄像头等高密度设备的并发需求，交换机接口从当前主流的 100G 向 400G/800G 升级。

AI 正逐渐成为推动园区网络变革的核心力量，Wi-Fi 设备、交换机等设备将内置算力芯片，配合 AI 驱动的园区网络控制器将在未来给园区网络带来如下变化：体验极致化、运维自治化、安全内生性。

未来园区网络的安全将经历从“被动防御”到“主动免疫”的范式转变，这一过程中，AI、量子计算、零信任架构等技术的深度融合将重塑安全防护体系。通过零信任架构、量子安全、数字孪生等技术构建“自学习、自防御、自适应”的智能安全体系。

物联融合已不仅是技术选择，而是园区从“物理空间”向“数字生命体”进化的必由之路。未来，通过物联融合，能够将园区内分散的设备、系统进行整合，实现数据的互通共享与协同联动，进而挖掘数据价值，为园区管理决策提供有力支撑，助力园区从单纯的设施管控向综合性的服务生态转型，极大地提升园区运营效率和服务质量，创造更大的价值。

综上，未来 3 到 5 年，Wi-Fi 的代际变化、AI、安全、物联融合等趋势将会成为园区网络发展的主旋律。

A

缩略语

表 A-1 缩略语

缩略语	英文全称	中文全称
GDP	Gross Domestic Product	国内生产总值
PC	Personal Computer	个人电脑
SLA	Service Level Agreement	服务水平协议
QAM	Quadrature Amplitude Modulation	正交幅度调制
AP	Access Point	接入点
VR	Virtual Reality	虚拟现实
AR	Augmented Reality	增强现实
AI	Artificial Intelligence	人工智能
VIP	Very Important Person	重要用户
SDN	Software defined Networking	软件定义网络
ETH	Extremely High Throughput	极高吞吐量
PPDU	Physical Layer Protocol Data Unit	物理层协议数据单元
RU	Resource Unit	资源单元
TCO	Total Cost of Operations	总成本
PHY	Port Physical Layer	端口物理层
PoE	Power over Ethernet	以太网供电
WLAN	Wireless Local Area Network	无线局域网
HTTP	Hypertext Transfer Protocol	超文本传输协议

缩略语	英文全称	中文全称
FTP	File Transfer Protocol	文件传输协议
QoS	Quality of Service	服务质量
RTT	Round Trip Time	往返路程时间
VoIP	Voice over Internet Protocol	基于 IP 的语音传输
SaaS	Software as a Service	软件即服务
POS	Point of Sale	销售点
AGV	Automated Guided Vehicle	自动引导运输车
EDCA	Enhanced Distributed Channel Access	增强型分布式信道访问
SRv6	Segment Routing over IPv6	基于 IPv6 的段路由
VXLAN	Virtual Extensible Local Area Network	虚拟扩展局域网
VLAN	Virtual Local Area Network	虚拟局域网
ZTP	Zero Touch Provisioning	零配置部署
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
LAN	Local Area Network	局域网
WAN	Wide Area Network	广域网
API	Application Programming Interface	应用编程接口
OUI	Organizationally Unique Identifier	组织唯一标识符
LLDP	Link Layer Discovery Protocol	链路层发现协议
ONVIF	Open Network Video Interface Forum	开放网络视频接口论坛
WPA	Wi-Fi Protected Access	Wi-Fi 保护访问
MIMO	Multiple-input Multiple-output	多输入多输出
SZTP	Secure Zero Touch Provisioning	安全零配置部署
CSI	Channel State Information	信道状态信息
ALS	Automatic Laser Shutdown	激光器自动关断

缩略语	英文全称	中文全称
EEE	Energy Efficient Ethernet	能效以太网
RFID	Radio Frequency IDentification	射频识别
MTTR	Mean Time To Repair	平均修复时间