宽带发展联盟
Broadband Development Alliance

Network Innovation and Development Alliance
全球固定网络创新联盟

世界无线局域网应用发展联盟
WLAN Application Alliance

高品质万兆园区网络技术发展研究报告

Network Innovation and Development Alliance

November 20, 2024

前言

随着新一轮科技革命和产业变革重构全球创新经济结构版图，以数字经济发展为代表的新技术新业态，正在推动人类社会进入数智化新阶段。

园区是政务、办公、制造、医疗、教育、交通等千行百业的主要活动场所，也在向数字化、智能化、融合化、安全及绿色低碳等方向演进。随着 AI（Artificial Intelligence，人工智能）和云技术的应用，远程办公的普及，以及高清 XR（Extended Reality，扩展现实）、裸眼 3D、虚实结合元宇宙等新业务的兴起，园区网络正处于从千兆园区网络向高品质万兆园区网络演进的阶段。

高品质的万兆园区网络不仅仅需要满足接入带宽的大幅提升，还需要具备无线网络的连续组网、应用和用户体验的提升和保障、网络运维智能、安全及绿色低碳等能力。高品质万兆园区的网络架构和技术都有较大的更新。

本文梳理并总结了园区的业务发展趋势，对园区网络的需求、无线 Wi-Fi 接入技术以及有线接入技术进行分析，提出高品质万兆园区建网方案、关键技术和关键指标，并给出分级指标建议。通过结合通信产业新技术发展和创新方向，支撑高品质万兆园区网络解决方案落地，推动园区网络向万兆超宽、确定可靠、体验保障、智能运维、安全防护、绿色低碳等方向发展，为企业园区数智化转型和产业升级提供强有力支撑。

本研究报告的参编单位有中国信息通信研究院、中国电子工程设计院股份有限公司、中国建筑东北设计研究院有限公司、华为技术有限公司、中兴通讯股份有限公司。本研究报告主要撰稿人有郭晓岩、李洪鹏、党梅梅、李少晖、陈洁、卢希、苗甫、袁立权、赵少奇、邱月峰、赵能钰、马安邦、朱航、张蓁、季晨荷、姜林、李大鲲、沈杰、翁财忍、韦乃文、张印熙、张婷、路程等。感谢所有的参编单位和撰稿人。

本研究报告也获得了中国勘察设计协会智能分会的大力支持，在此一并感谢。

目 录

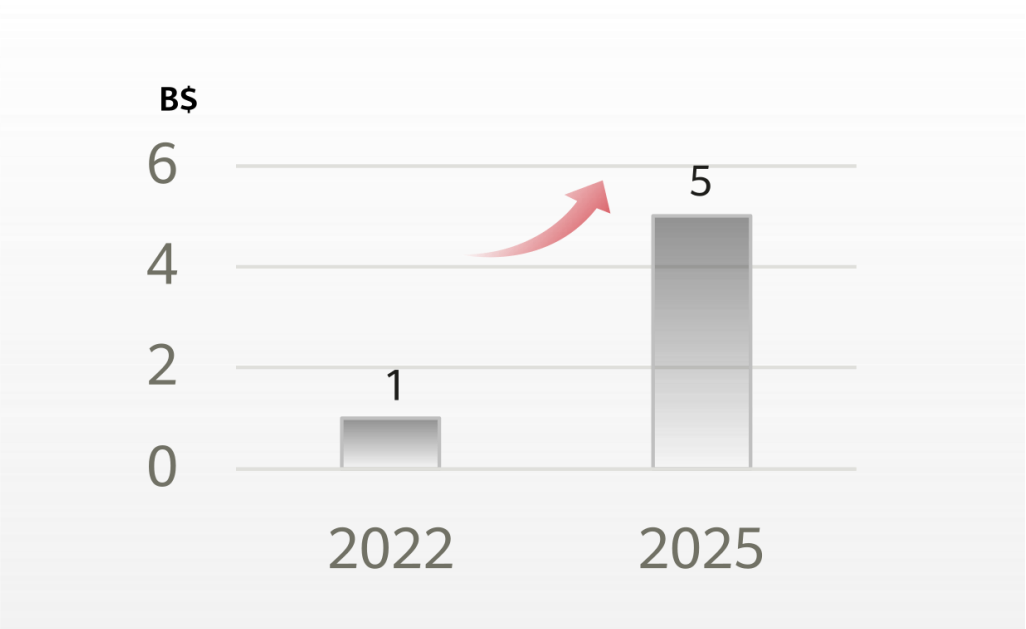
1 园区业务发展趋势

园区作为城市的基本单元，是最重要的人口和产业聚集区，埃森哲联合华为发布的 《未来智慧园区白皮书 2020》指出，园区覆盖了绝大部分工作生产场景，80%以上的 GDP 和 90%以上的创新在园区内产生，因此可通过园区业务发展趋势分析作为园区网络演进趋势分析的基础，园区业务具有以下发展趋势：

1. 终端数量快速提升

接入到网络中的终端主要包含两类，一类是智能终端，包含个人电脑（Personal Computer，PC）、手机等。根据 Gartner & ABI Research 权威机构统计和预测，人均无线终端数量将从 2022 年的人均 1 台增加到了 2025 年的人均 3～5 台。

图1-1 人均终端数目变化趋势



Source： Gartner & ABI Research

另一类是物联终端。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，扣除智能手机、平板电脑、笔记本电脑或固定电话等连接之外，物联网设备的数量已达到 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%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；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，且这个变化趋势在园区网络中更加明显。

图1-2 全球联网设备的数量已达到了 170 亿

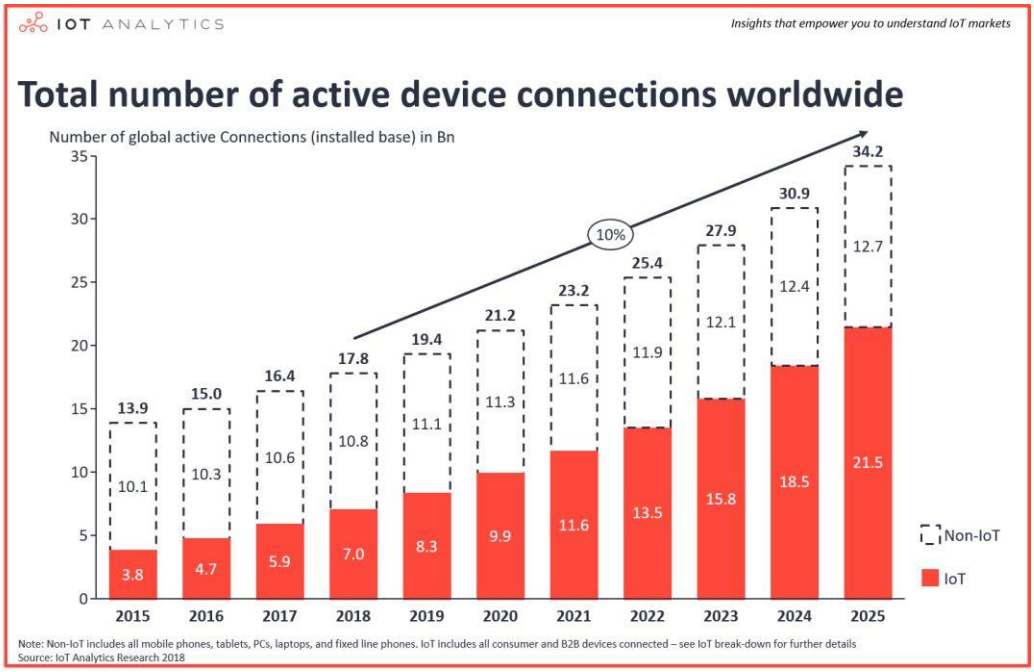
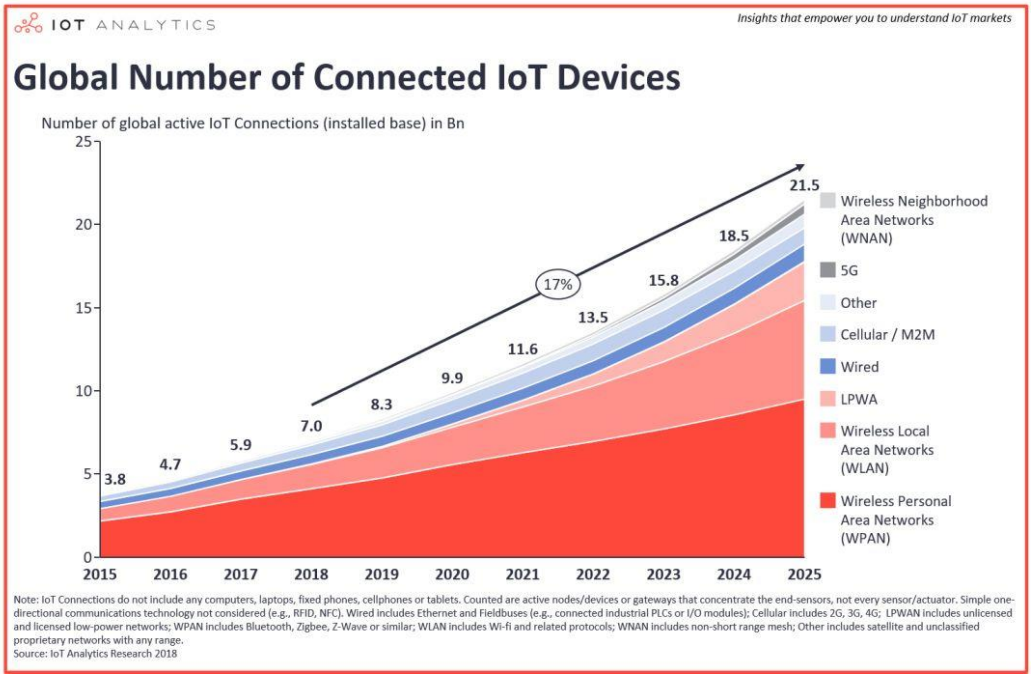


图1-3 全球物联设备中 80%为无线方式，且以 17%的年增长率增长

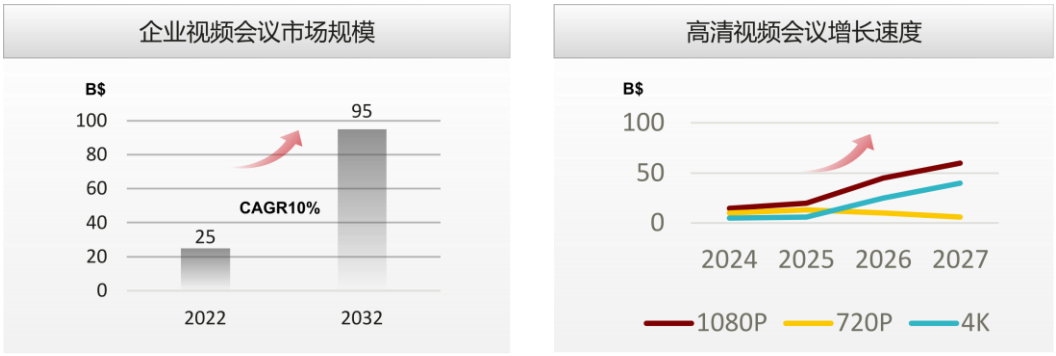


2. 无线业务带宽快速增长

企业办公业务中，云桌面、视频会议、4K 视频、新一代的 VR（Virtual Reality，虚拟现实）、AR（Augmented Reality，增强现实）、虚拟助手等应用逐渐普及，对带宽的需求激增。以视频会议为例，视频

会议作为企业远程沟通和混合办公的重要工具，全球市场规模在未来 10 年将增长近 4 倍，复合年均增长率达到 10%，其中高清视频会议市场是关键增长点。视频会议市场规模与视频会议数量之间呈正比，这意味着园区网络需要支持成倍增长的视频会议流量。

图1-4 视频会议变化趋势



Source：Gartner & ABI Research

3. 确定可靠是制造生产网络的刚需

随着企业数字化转型的不断深入，智慧工厂的架构逐渐清晰。企业数字化转型的本质是借助不断进步的 ICT 技术（Information and Communications Technology，信息和通信技术）将末端设备/机器实现数字化，真正实现让设备“开口说话”，让机器作业代替人工作业。随着 ICT 技术的进一步发展，部分企业也开始向智能化方向转型，用 AI 实现数据训练和数据分析处理，实现工厂生产的无人化、智能化。自动化生产线和智能机器人需要具备运动周期的精确控制和高可靠的冗余保护能力，因此对园区网络的确定性和可靠性提出了更高的要求。

4. 业务体验需求更明确

园区内音视频会议、VR、AR 等时延、抖动敏感型业务持续增长，对园区网络提出了更高要求。比如视频会议对时延的要求一般小于 150ms，抖动小于 50ms，因此需要网络提供更稳定的质量保障。而正在快速增长的 VR 业务对带宽和时延要求更高：单连接带宽要求超过 500M，延迟不能超过 20ms。

5. 智能化运维成为共识

传统园区场景下，网络问题需要运维人员到现场进行处理，但随着园区部署区域越来越广、网络规模越来越大，且网络业务越来越复杂，人工现场运维方式难以为继，需要为园区网络提供智能化运维能力，从对问题的被动响应向主动运维变革，以应对新的挑战。

6. 网络安全是园区的基石

未来随着园区无线网络的建设与推广，以及 VPN（Virtual Private Network，虚拟专用网络）等远程接入技术的成熟应用，企业员工的办公位置变得更加灵活，企业园区网络的物理边界会逐渐消失。同时物联网和车联网的快速发展，使得越来越多的 IoT 设备接入网络，形成了庞大的物联网生态系统，但这些设备的安全防护能力参差不齐，很容易成为黑客的攻击目标。这些变化都导致园区对网络安全的诉求更加强烈。

7. 绿色低碳成为新方向

全球气候变化的影响正对全人类生存发展带来重大挑战，主要国家和地区纷纷加速向碳中和迈进。英国在 2019 年修订了《气候变化法案》，正式确立了到 2050 年实现温室气体“净零排放”的目标。欧盟正在立法要求 2050 年实现碳中和。南非承诺 2050 年实现碳中和。2021 年 10 月 26 日，中国国务院印发《2030 年前碳达峰行动方案》，确定 2030 年前碳达峰目标，对推进碳达峰工作做出总体部署。实现碳达峰、碳中和是一场广泛而深刻的经济社会系统性变革，这些变革也推动着园区的绿色低碳技术革新。

基于上述园区业务发展趋势分析，具备万兆超宽、确定可靠、体验保障、智能运维、安全防护和绿色低碳特征的高品质万兆园区网络，将成为园区网络发展的必然趋势。

下面将针对上述园区业务发展趋势，进一步分析对园区网络的需求。

2 园区网络需求分析

2.1 万兆超宽需求

新型办公应用对网络带宽提出更高要求

基于多家企业和机构（Huawei, Cisco, Microsoft, Frontier Communications,HealthIT.gov）的调研数据情况分析，4K/8K 视频、实时影像、在线游戏、高清视频会议、VR/AR 等新业务都需要更大的网络带宽。

表2-1 业务对带宽的要求

业务	带宽
4K 高清视频/Streaming Ultra HD (4K) video	15~30 Mbps
8K 高清视频/Streaming Ultra HD (8K) video	40~100 Mbps
实时影像（医疗）/Real-time imaging (healthcare)	≥30Mbps
在线游戏/Online gaming	3~6 Mbps
高清视频会议/HD video conferencing	5~7.2 Mbps
标准 AR 及 VR（娱乐）/ Standard AR&VR (entertainment)	≥30 Mbps
增强 AR 及 VR（培训）/Advanced AR&VR (training)	>80 Mbps
极致 AR 及 VR（远程手术）/ Perfect AR&VR (remote surgery)	≥1.5 Gbps

无线终端成倍增长要求网络接入能力提升

随着智能终端的普及，人们对智能终端的依赖度越来越高，每人至少一个智能手机，部分人员有两个手机或者外加一个平板电脑。而随着无线化的普及，办公便携也从传统的台式机演变为笔记本，还有一些辅助办公设备，比如无线话机、无线打印机等。以办公室为例，平均每人终端数达到 3~4 个，假设一个 AP 覆盖 15~-20 人的区域，则原本一个 AP 连接 15~20 个终端，演变为 45~60 个终端，AP 的接入密度有了 3~4 倍的提高。

在办公园区不同的场景下，网络承载的主要应用类型以及接入终端数量不同，因此对网络的要求也不一样，以高清会议区为例，当一个 AP 下挂有 30 个用户进行 4K 高清视频会议的时候，需要无线网络提供约 450Mbps~1.5Gbps 的带宽，如表 2-2 所示：

表2-2 不同场景对无线网络的要求

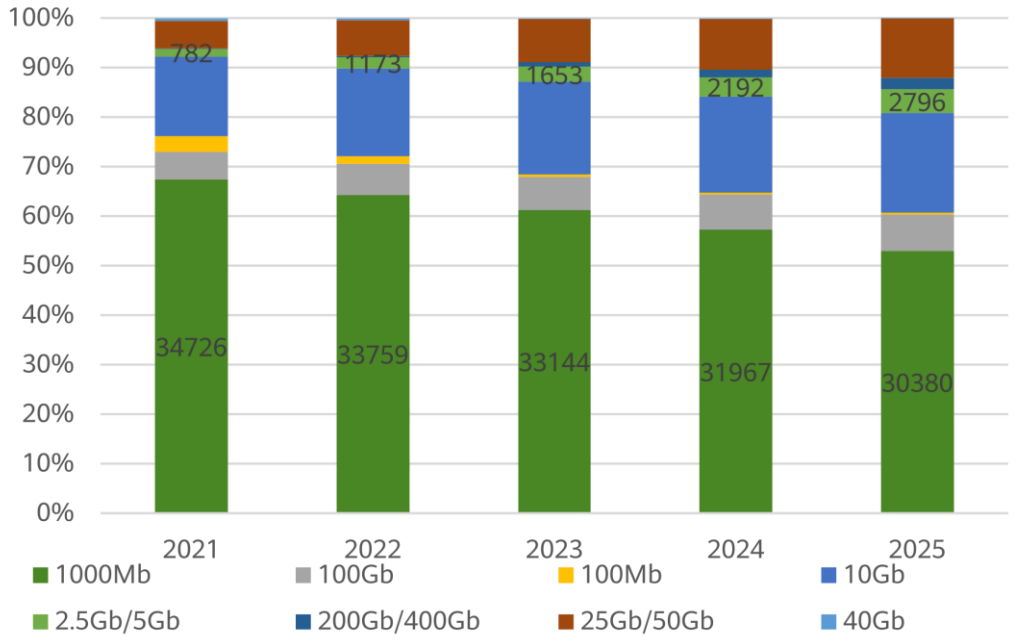
场景	应用	带宽	时延	终端数	带宽诉求
高清会议区	720P	2Mbps	40ms	30~50	60Mbps~100Mbps
	1080P	5~7.2Mbps	20~40ms	30~50	150Mbps~360Mbps
	4K 视频会议	15~30Mbps	20ms	30~50	450Mbps~1.5Gbps
研发办公区	AI 协同办公	500Mbps	10~20ms	15~30	7.5Gbps~15Gbps

有线终端接入带宽提升

为了适应新型应用对网络高带宽的诉求，终端侧各大主流厂商已经广泛推出支持 2.5GE/5GE 网卡的电脑。另外超薄笔记本的网卡转换器 USB/Type-C 转 2.5GE 也成为主流方案之一。

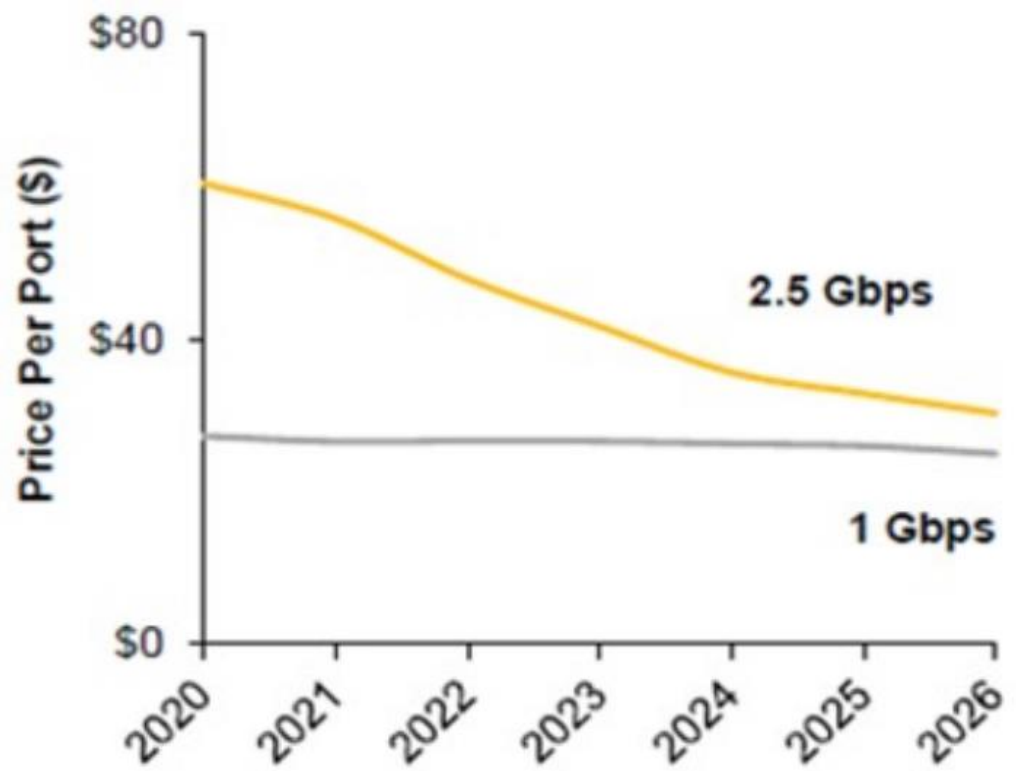
从 IDC 发布的全球支持 GE 或 2.5GE/5GE 端口的网络设备和终端发货量看，到 2025 年支持 2.5GE/5GE 的网络设备和终端发货量将超过支持 GE 端口的网络设备和终端的发货量，成为市场的主流。

图2-1 GE 和 2.5GE 端口发货量变化



权威机构 DELL'ORO 也发布了端口增长预测，2.5GE/5GE 端口将出现高速增长，每年增长率翻倍。预计 2.5Gbps 交换机的端口出货量将从 2021 年的 80 万增长至 2026 年的 3900 万，DELL'ORO 也对端口成本的变化进行了预测，随着产业链的催熟，2.5GE 产业链的成本会越来越低，预测 2025~2026 年 2.5GE 单端口价格和 GE 单端口价格差不超过 20%，这将进一步促进 2.5GE 使用量的增长。

图2-2 GE 和 2.5GE 端口成本变化



2.2 确定可靠需求

工业领域的自动化控制、自动化生产等场景，在数据传输的时延、抖动、可靠性等方面提出更高要求。

- 控制系统中，现场级的自动化控制系统对数据传输时延要求非常严格，在一些高精度机床上的运动控制指标要求达到 1ms 以内。生产网络中，同步实时流对时延的要求最高，该流量周期性发包，一般发包周期小于 2ms；每周期发送的数据长度相对稳定，一般不超过 100Bytes；端到端传输具有 deadline 要求，即数据需要在特定的绝对时间之前抵达对端。
- 精密制造工厂内制造设备和主机服务器之间，以及工厂内系统之间均存在大量单播或组播消息，消息交互非常频繁，对网络的连续性、可靠性要求高，对网络的智能化运维排障诉求强烈。业界专家预测，半导体工厂一旦生产停工，会造成巨额损失（据典型测算，停工 30 分钟，损失 5000 万美元，平均每秒损失 2.6 万美元），因此需要建设零中断的生产网。工业现场的控制业务往往都在毫秒级，保护倒换要求更快，甚至要达到亚毫秒级。业务诉求不满足会导致生产业务连接中断，影响生产节拍，从而造车生产效率降低，造成企业的经济损失。

表 2-3 为 3GPP 定义的工业场景中 CT（Cycle Time，周转时间）、抖动等要求，核心的工业场景均需要确定性时延支撑，时延要求越高的业务，对应的可靠性要求也越高。

表2-3 3GPP 定义的工业场景关键指标

类型	场景	周转时间	带宽	抖动	可靠性
运动控制	大型打印机	< 2 ms	>8 Mbit/s	1 μ s	99.9999%
	数控车床	< 0.5 ms	>16 Mbit/s	1 μ s	99.9999%
	包装设备	< 1 ms	>16 Mbit/s	1 μ s	99.9999%
机器间控制（C2C）	多台独立机器间协作	4~10ms	/	1 μ s	99.9999%
移动面板带安全控制	装配机器人（或机床）	4~8ms	/	50%*CT	99.9999%
		<30ms	>5 Mbit/s		
	移动式起重机	12ms	/	50%*CT	99.9999%
工业 AR 及监控	高清（1280×720）	10ms	1.33 Gbit/s	/	99.9%
	全高清（1920×1080）		3 Gbit/s		
大规模连接	基于安全应用	5~10ms	100 Mbit/s	10%*CT	99.9999%
	基于事件应用	50ms~1s		/	99.9%
	基于区间应用	50ms~1s		/	99.9%
移动机器人	精准运动控制	1ms	/	50%*CT	99.9999%
	机器间控制	1~10ms	/		
	协作驾驶	10~50ms	/		

2.3 体验保障需求

为了提升业务和用户体验，需要支持应用可视、应用保障、应用质量检测、定位，以及 VIP（Very Important Person，重要用户）体验保障优先能力。

应用可视

园区内的应用越来越多，需要能直观看到应用的种类和应用的流量分布，网络设备需要支持应用识别的能力，预置业界常用的应用识别能力，同时通过自定义应用能力实现对企业内部私有应用的识别。

应用保障

为了保障 4K/8K 视频、实时影像、在线游戏、高清视频会议、VR/AR 等新业务良好的使用体验，除了对网络带宽有诉求外，对网络时延也提出了要求，如表 2-4 所示：

表2-4 不同业务的网络时延要求

业务	时延
4K 高清视频/Streaming Ultra HD (4K) video	20 ms
8K 高清视频/Streaming Ultra HD (8K) video	20 ms
实时影像（医疗）/Real-time imaging (healthcare)	≤200 ms
在线游戏/Online gaming	20~40 ms
高清视频会议/HD video conferencing	20 ms
标准 AR 及 VR（娱乐）/ Standard AR&VR (entertainment)	≤20 ms
增强 AR 及 VR（培训）Advanced AR&VR (training)	15 ms
极致 AR 及 VR（远程手术）/ Perfect AR&VR (remote surgery)	≤8 ms
Sources: Huawei, Cisco, Microsoft, Frontier Communications,HealthIT.gov	

另外 IETF（Internet Engineering Task Force，互联网工程任务组）对园区应用的丢包、时延、抖动指标给出了定义，容忍度不同推荐的 DSCP 值也不同，具体值参见如表 2-5 所示：

表2-5 DiffServ 服务等级的配置原则举例（RFC 4594）

业务分类	业务特征	应用举例	丢包容忍度	时延容忍度	抖动容忍度	优先级	DSCP 值
多媒体会议	桌面多媒体会议（仅包括语音和视频，其数据归到 Low-Latency Data 类）	H.323/V2 视频会议（自适应）	低-中	非常低	低	AF41 AF42 AF43	100010(34) 100100(36) 100110(38)
实时互动	视频会议（仅包括语音和视频，其数据归到 Low-Latency Data 类）、高清视频、交互式游戏(使用 RTP/UDP)	视频会议和交互式游戏	低	非常低	低	CS4	100000(32)
多媒体流	VoD 视频点播	流媒体视频和音频点播	低-中	中	是的	AF31 AF32 AF33	011010(26) 011100(28) 011110(30)

业务分类	业务特征	应用举例	丢包容忍度	时延容忍度	抖动容忍度	优先级	DSCP 值
低时延数据	交互式的重要数据业务，要求响应时间短，如 VCX IP 消息业务、ERP、CRM、DB	客户端/服务器交易基于 Web 的订购	低	低-中	是的	AF21 AF22 AF23	010010(18) 010100(20) 010110(22)
运维管理	网络运维、维护和管理业务，例如 SNMP、Syslog、SSH	OAM & P	低	中	是的	CS2	010000(16)

但应用发出报文的优先级经常和推荐的不同，导致报文在网络传输中无法得到保障。因此，需要网络支持基于应用调整应用流量优先级，保障关键应用优先转发，减少丢包和时延。通过对部分应用进行分析，应用实际使用的优先级如表 2-6 所示：

表2-6 应用默认优先级举例

应用	终端类型	优先级
Zoom	win10 PC	AF31(26)
	win10 Laptop	AF31(26)
Microsoft Teams	win10 PC	EF(46)
腾讯会议	win10 Laptop	EF(46)
华为云会议	win10 PC	AF11(10)
	win10 Laptop	AF11(10)
钉钉会议	win10 Laptop	CS6(54)

在分支园区互连场景下，首先为了保障应用始终运行在最优的网络链路中，需要支持基于最优路径的动态选择。同时为了保障在部分链路故障时，不依靠重传来保证应用质量，还需要支持冗余收发报文技术。

应用质量检测和定界

应用丢包不可避免，网络需要提供随流检测的能力，监控关键业务流在网络途径设备的 SLA（Service Level Agreement，服务水平协议）。当故障发生后，可以快速定位到故障发生在哪台设备以及故障产生的原因。

VIP 体验优先

在园区中，VIP 除了企业重要用户，还包括接入网络的重要终端，比如会议室中的视频会议终端、商场的 POS 机、工厂的 AGV 小车。在高密、弱信号、频繁移动等无线场景下，通过 VIP 优先的策略，对 VIP 提供高速率、低时延的无线接入网络，为 VIP 提供万兆高品质网络体验。

2.4 智能运维需求

IDG 的数字化商业转型状况报告指出，52%的高管认为“成为数字化业务意味着通过移动、数据访问和辅助流程等工具来提高员工的生产率”。接近一半的高管(49%)，也将数字化转型视为“通过数据可用性和可见性更好地管理业务表现的能力”。对于 46%的决策者来说，数字化转型意味着满足客户体验期望，另外有 44%的人认为这意味着可以通过数据收集和分析来理解客户需求。

由于终端类型、操作系统类型、业务类型、流量模型的持续多样和复杂化，导致传统的“以设备为中心，以命令行为手段”的“逐跳排障”式人工运维越来越困难。传统运维方式主要是在问题发生后进行排障处理，这种事后运维模式无法应对数字化业务带来的挑战。同时数字化场景对故障的处理和恢复时间的容忍度在降低，比如医疗自动分药系统、商业无人支付系统、仓储自动导引运输车（Automated Guided Vehicle，AGV）等场景对故障的处理和恢复时间的容忍度远低于普通办公业务。

部署自动化

应包含设备即插即用自动上线、基于意图的自动化业务布放，以及可灵活定制满足不同场景的自动化部署等能力。

网络可视化

智能运维工具需要具备在实时获取网络、用户、应用信息的基础上，自动生成网络、用户、终端、应用的可视化界面的能力，便于运维人员更直观的监控和管理网络。类似于在城市交通活动中人们需要“高德地图”查询位置、导航、看路况、了解道路拥塞原因，网络世界同样需要一张高精度的“网络数字地图”，轻松洞悉园区网络、用户、应用的体验旅程，为智慧园区极致体验保驾护航。

定位智能化

园区网络存在多类业务节点和网络节点，这些不同的节点、不同的指标之间存在很多关联，使得网络的故障模式是复杂和多变的。针对同一个问题现象（比如用户认证失败）可能有不同的根因（弱覆盖、证书错误），而不同的现象（带宽低体验差、信道利用率高）可能指向相同的根因（区域干扰）。通过智能分析器可对海量数据进行关联性分析，找出未知的关联和因果关系，从而有效地帮助运维人员寻找无线覆盖、用户认证失败、二层环路等问题的原因。

调优自动化

智能运维工具需要支持收集和分析大量网络数据，通过机器学习算法，持续学习并适应网络环境的变化，通过预测性算法，提前预测问题，并启动自动化流程进行响应，快速纠正问题，降低网络问题发生的可能性。

LAN&WAN 融合

在业界现有的网络管理解决方案中，LAN（Local Area Network，局域网）和 WAN（Wide Area Network，广域网）维护是分开的。维护团队需要采取两个运维系统，两个策略，两个维护团队，这些大大提高了 IT 部门的 OPEX（Operating Expense，运营支出）。为了提高运维效率，需要 LAN&WAN 融合的网络管理系统。通过融合平台，一个平台可以提供跨域可视化，提升管理体验。同时还可以支持策略协同，优化从广域网到局域网的应用体验。

2.5 安全防护需求

园区网络安全面临的挑战是多方面的，这些挑战随着技术的发展和网络应用的普及而不断演变。万兆园区需要具备更高安全防护的能力。

终端安全

接入网络需要满足以下诉求，从而保证各类终端能够“极简”“安全”的接入到园区网络：

- **终端全可视**：终端可视是网络安全的基础，终端如果不可视，就无法得知危险源的所在，容易造成网络安全漏洞，被黑客轻易攻击全网。
- **基于终端类型安全接入**：在企业办公园区网络中，由于各类哑终端入网认证能力参差不齐，MAC 认证仍然是当前主流的哑终端入网认证方式。然而海量哑终端的 MAC 采集录入已成为影响终端入网效率的关键因素，因此园区网络需要一种可免采集 MAC 地址的极简入网方案。同时网络应提供根据不同终端类型，自动分配不同网络权限的能力。
- **终端防仿冒/防私接**：仿冒和私接问题是园区的主要安全问题，因此园区网络需具备基于终端类型防仿冒能力，可即时发现即时隔离相同 MAC 地址终端类型变更的安全问题。

链路安全

- **无线空口安全**：无线空口的 Wi-Fi 电磁信号通过天线在空间辐射，非法用户可以通过无线侦听抓包等技术抓取用户报文。为了防止数据被窃听，无线空口不仅需要支持对数据报文进行加密的能力，还要具备防止数据被抓取的能力。
- **有线安全**：需要提供包含 LAN 和 WAN（Wide Area Network，广域网）的端到端的数据加密能力。

出口安全

随着园区网络承载的重要业务越来越多，外部对园区内部的攻击也越来越多，因此园区网络需要具备防范来自互联网的流量过载、病毒、未知威胁文件攻击、数据窃取等攻击的能力。

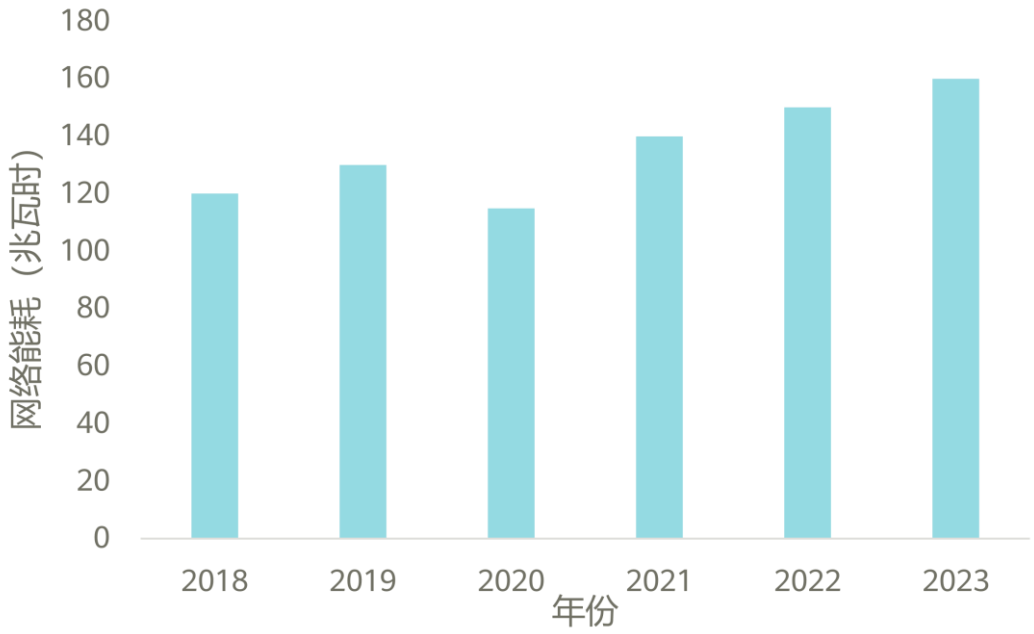
设备安全

设备在运行及软件升级过程中可能被黑客恶意攻击并非法篡改，恶意篡改后的软件、补丁或配置文件一旦运行可能造成用户信息泄露、系统资源耗尽、甚至会导致系统完全被攻击者控制，因此设备本身需要具备校验启动文件合法性和防护非法控制的能力。

2.6 绿色低碳需求

根据通信世界网研究表明，园区楼宇公共用能以建筑空调、照明、网络设备用能为主，其中网络设备需要 7*24 小时运行，能耗占比接近 15%，需要网络设备流量不断增加时能耗不增加。图 2-3 是近 5 年的园区网络能耗趋势。

图2-3 2018 年到 2023 年园区网络能耗趋势



园区网络绿色低碳是园区可持续发展战略中的重要组成部分，旨在通过优化网络架构、采用节能技术和管理手段，降低网络设备的能耗，提高能源利用效率，减少对环境的影响。园区网络设备除了自身具有节能的能力，整个网络还需要具有从网络架构和网络系统角度节能的能力。同时为了有效的评估网络节能的效果，对后续的节能手段进行指导，网络还需要有对网络能耗进行呈现的能力。

3 万兆园区无线 Wi-Fi 技术方案

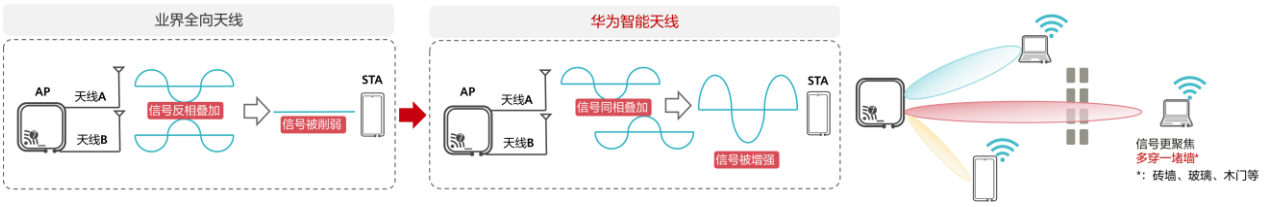
3.1 零盲区全覆盖

通过合理的网络规划能够有效减少覆盖盲区，但是在一些存在障碍物的场景中，信号经过遮挡后会导致覆盖效果变差，从而影响用户体验，智能天线技术能够有效解决这个场景下的问题。另外网络中的终端具有潮汐效应，动态变焦智能天线技术能够让 AP 设备根据用户数量的变化动态调整覆盖范围。

智能天线

一般企业 AP 采用的都是内置全向天线，天线增益有限，对近距离用户可以提供较好的服务，对于中远距离的用户只能提供较低吞吐量的服务。在实际组网中，障碍物遮挡也是对 AP 覆盖能力的挑战。典型的障碍物场景包括用户被柱子或墙遮挡。除此之外，在高密组网环境下，多用户并发将导致 AP 间干扰大大增加。如图 3-1 所示，智能天线能够显著提升覆盖和抗干扰能力，在相同的点位下性能相比内置天线提升 20%以上，相同信号强度较普通内置天线覆盖远 20%。同时当智能天线算法选择接收终端增益最大的波束传输下行信号时，通过定向波束的高增益，可以克服干扰信号的影响，实现下行用户传输的抗干扰能力。

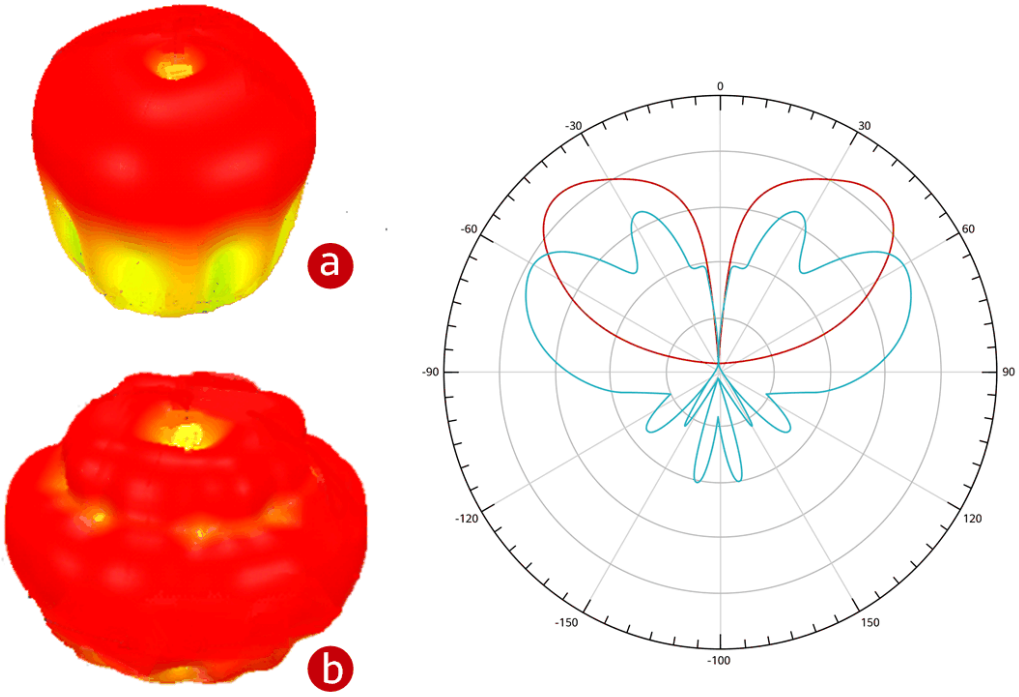
图3-1 智能天线



动态变焦智能天线

动态变焦智能天线（全向/高密模式合一天线），支持全向/高密模式可切换。在 AP 部署较为密集的区域（AP 间距小于 10 米），设置为高密模式可以降低同频 AP 之间的相互感知的信号强度，而不影响中心区域的覆盖能力；在 AP 部署较为稀疏的区域，可切换回传统全向模式，可保障单个 AP 覆盖范围尽可能大。如图 3-2 所示，一款 AP 同时支持全向/高密两种模式，随着场景中终端的潮汐变化，智能选择相应的模式，在高密模式下抗干扰能力提升 6dB，整网性能提升 20%。

图3-2 动态变焦智能天线潮汐变化图



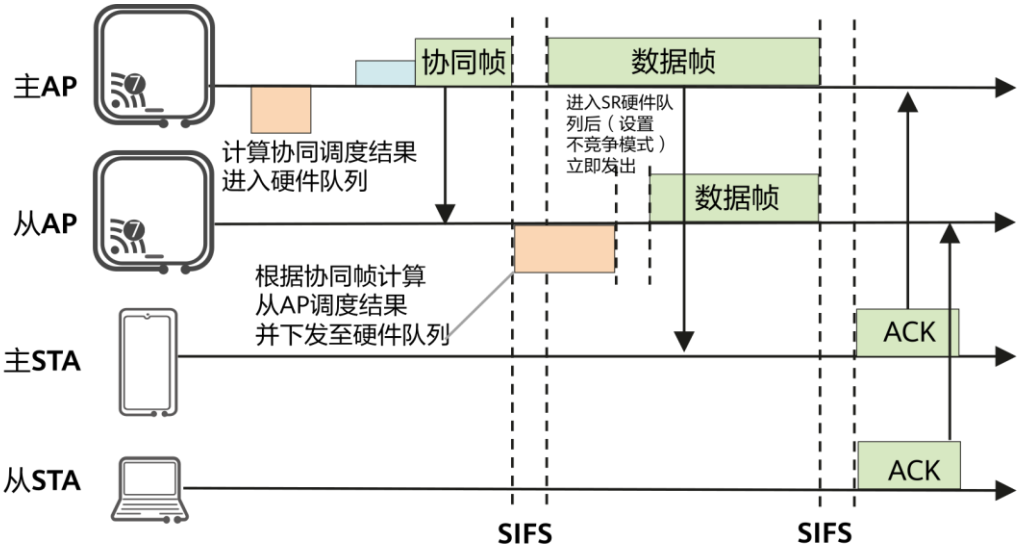
3.2 智能无线调优

无线网络调优是一个系统工程，传统的调优技术通过建立 AP 之间的逻辑拓扑，对 AP 的功率和信道进行调整。同频部署的 AP 没有协同工作，导致同频干扰比较严重。同时网络在调优计算时并没有考虑 AP 高挂、遮挡等场景，也没有考虑网络中的历史干扰和负载信息，导致实际调优效果并不理想。

多 AP 干扰协同

在 Wi-Fi 6 及其之前的 802.11 协议框架内，AP 之间实际上没有太多协作的关系。自动调优、智能漫游等常见的 WLAN（Wireless LAN，无线局域网）功能都属于厂商自定义特性，AP 间协作也仅仅是优化信道选择，调整 AP 间负载等，以实现射频资源高效利用的目的。如图 3-3 所示，Wi-Fi 7 标准中多 AP 间的协同调度可以有效降低 AP 之间的干扰，极大的提升空口资源的利用率。

图3-3 多 AP 干扰协同示意图



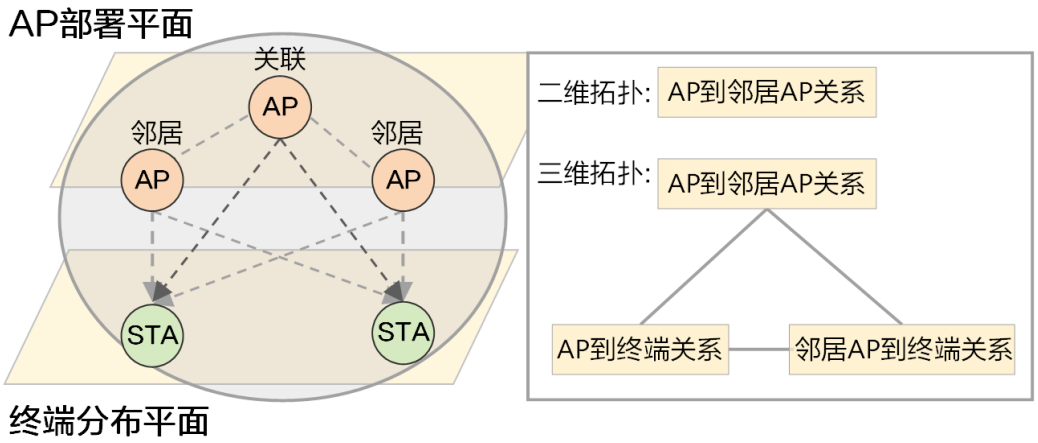
注：此处主 AP 是负责 AP 之间协同调度计算的 AP，其对应连接的 STA 定义为主 STA。

立体射频调优

本质上 WLAN 网络是一个 AP 和终端共同组成的三维空间。单靠 AP 间的测量，只感知到了平面的二维拓扑，缺少对三维复杂空间环境的考虑，而现实空间中各种遮挡、高挂等环境带来的信号折射/反射/衰减等情况，都会影响 AP 到终端的信号传播效果，导致在一些复杂环境中调优结果不理想。

立体射频调优功能借助对终端的下行测量，构成一个三维立体的拓扑关系，如图 3-4 所示，能够全面真实的反映无线信号在空间中传播的情况及信号对终端和 AP 的影响。以三维拓扑为基础的立体射频调优也能更好地适应复杂多变的空间环境，提升整体的调优效果。

图3-4 立体射频调优示意图



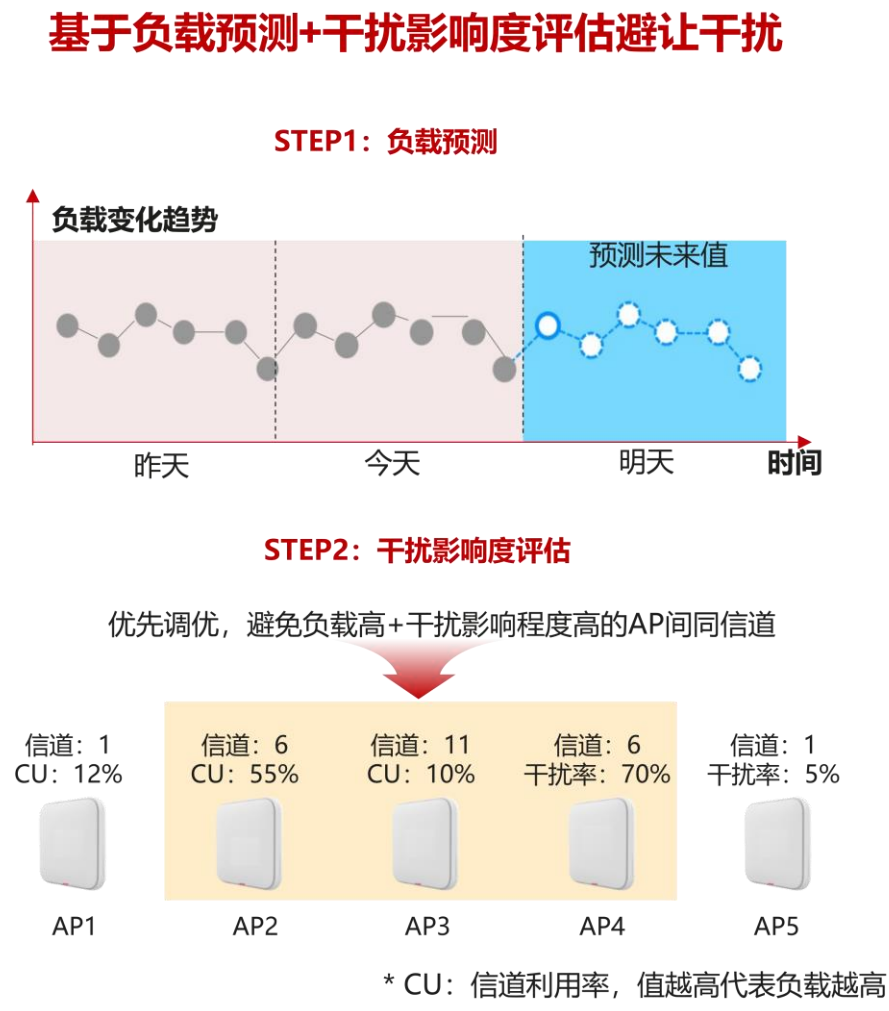
通过立体射频调优，可识别常见的 AP 间遮挡场景，避免由于遮挡出现严重的同频干扰。同时，针对 AP 高挂场景优化可以适应实际部署的各种特殊情况，包括层高过高、天花板安装、覆盖范围过大等，以满足覆盖需求优先，尽量保证 90%的用户处在良好覆盖区域。

智能无线射频调优

传统的基于射频探测感知周围环境而进行的调优，是一种周期性、被动的调优方式，采集的主要是射频干扰信号，而对实际的业务情况考虑比较少，并且网络在凌晨时段触发定时调优，仅能基于当时的网络状态调优，无法感知白天繁忙阶段 AP 真实的业务负载，以及白天周期出现的固定干扰源，网络调优的效果难以保证，无法充分利用射频资源。理想的调优模式需要考虑网络中的负载，智能预测网络中的用户数、流量，并结合历史数据，计算出最优的网络射频参数，保证空口能达到最优的收发效率。

如图 3-5 所示，智能无线射频调优方案利用大数据平台分析设备上报的大量数据信息，准确识别网络的拓扑和边缘 AP 设备，通过对历史数据的分析预测下一个调优周期内的负载。系统启动调优时，以最新的预测数据作为调优算法的输入值，结合实时的网络质量进行调优计算，从而获得最优的调优效果。

图3-5 智能无线射频调优示意图



3.3 智能漫游切换

传统漫游方案由终端主动漫游进行切换，存在如下问题：

1. 由于 Wi-Fi 是起源于家庭场景，几个房间只有 1 个 AP，导致部分终端厂商的漫游特性趋于保守，尽量不漫游。
2. 终端主动漫游时，全信道扫描耗时较长，找不到合适的目标 AP，导致切换时机偏慢。
3. WLAN 协议标准约束性不强，由于协议兼容性和软件实现原因，导致各类终端的漫游过程，漫游门限，协议支持能力参差不齐。

为了提升终端漫游体验，需要智能漫游技术帮助网络对终端进行差异化漫游引导。如图 3-6 所示，智能漫游核心逻辑是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；由终端“千端一面”变为“终端画像”，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3-6 智能漫游切换示意图

终端使用 AI 漫游引导速率提升 70%，整网的终端平均 RSSI 相较普通漫游提升 5dB 以上，漫游过程中带宽提升 30%，达到无缝漫游、无感切换效果。

3.4 关键指标

无线技术性能指标以《T/WAA 013—2024 园区办公场景 WLAN 性能技术规范（基于 802.11BE）》为准，部分指标如表 3-1 所示。

表3-1 Wi-Fi 7 网络关键指标

分类	指标项	吞吐量指标
带宽	单用户极限（5G，160MHz，下行）	≥2000Mbps
连接	30 用户总吞吐（5G，160MHz，下行）	≥1000Mbps
覆盖	5m 覆盖性能（5G，160MHz，下行）	≥1620Mbps

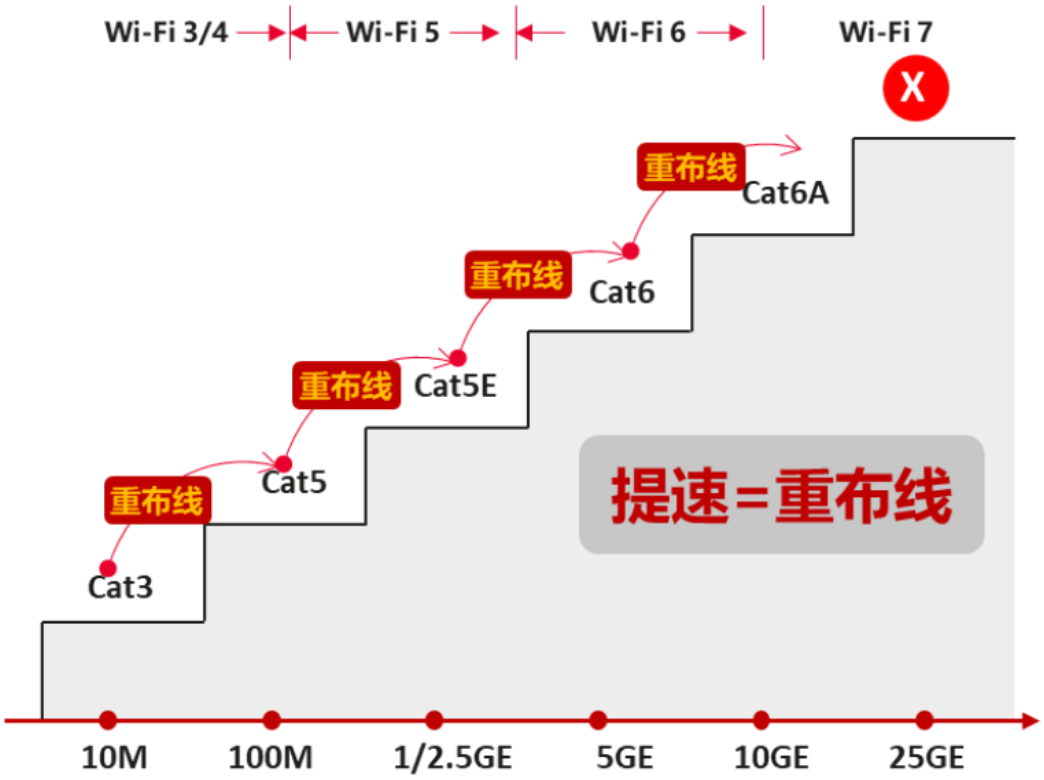
4 万兆园区有线技术方案

4.1 经典万兆以太网

用于连接终端和接入交换机的网线代际分明，带宽从 Cat5 的 100Mbps，Cat5E 的 1Gbps，到 Cat6 的 2.5Gbps/5Gbps，再到当前 Cat6A 的 5Gbps，Cat7 的 10Gbps，每一次网络带宽的升级都会伴随着网线的翻新升级改造，会造成较大的投资浪费。因此园区网络设计需要综合考虑利旧现网布线、成本最优和长期演进等几方面因素：

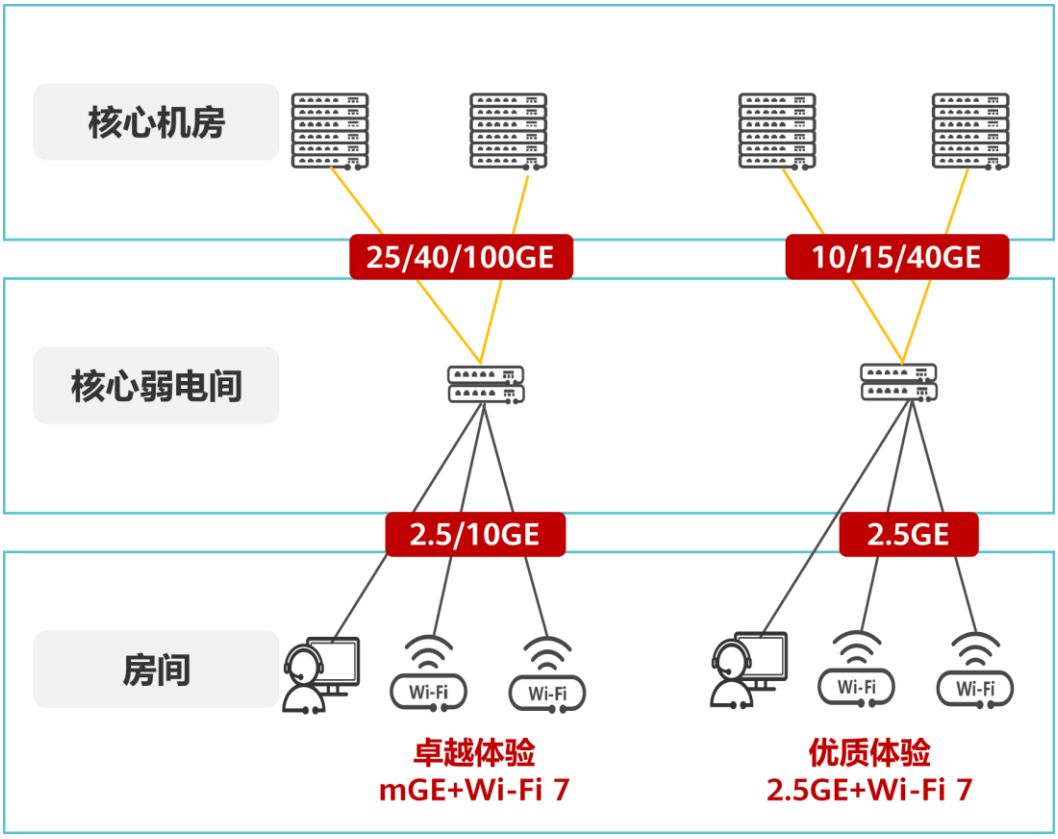
- 现网广泛部署的 Cat5E/Cat6 类线缆可满足 GE 升级到 2.5G 速率，因此 Wi-Fi 6 到 Wi-Fi 7 升级无需更换线缆，免重复布线，TCO 可节省 30%。
- 超过 2.5G 速率的场景，由于 5GE/10GE 在成本和功耗相同，产业界 PHY（Port Physical Layer，端口物理层）只提供唯一芯片，因此建议一般都是采用 10GE 兼容 5GE 的方式规划建设。

图4-1 网线代际分明，每次提速都需翻新线缆，成本高



在经典以太组网架构中，可以看到两种组合，分别是三射频 Wi-Fi 7 采用 5GE/10GE 上行，和两射频 Wi-Fi 7 采用 2.5GE 上行，配合不同速率的交换机，可以构建优质体验的 2.5GE 组网和卓越体验的 10GE 组网。对于配套 Wi-Fi 7 初步的无线体验及利旧 Cat5E/Cat6 布线场景采用 GE/2.5GE 组网，面向高端办公和高密场景可部署卓越越体验 10GE 组网，AP 支持 3 射频，整机速率高，上行带宽大。建议部署 Multi GE 组网，支持 2.5GE 平滑升级到 10GE 能力，以节约整体成本和支持长期演进。

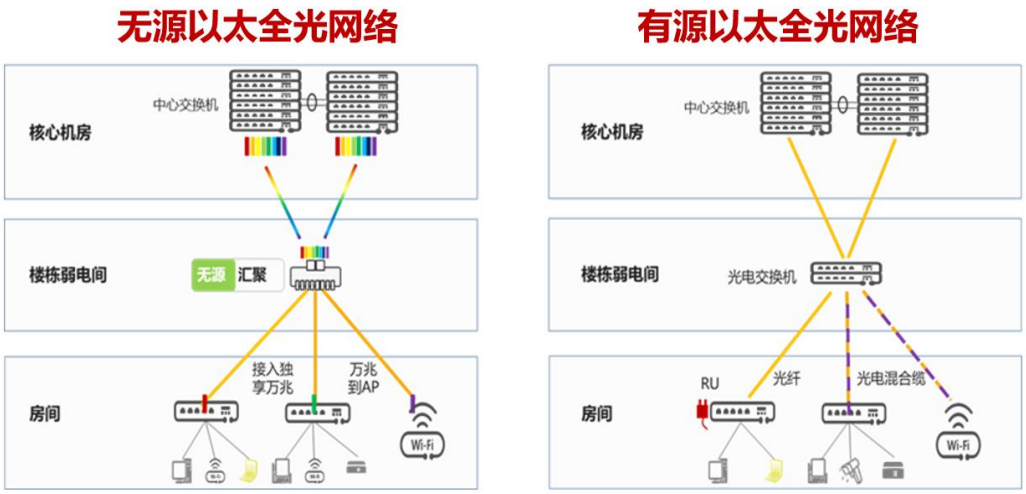
图4-2 万兆以太网组网图



4.2 万兆以太全光网

基于万兆到房间、全光到房间的以太统一架构方案，可提供极简架构、平滑演进的能力，万兆以太全光网络包括无源和有源两种方式。

图4-3 万兆以太全光网组网图



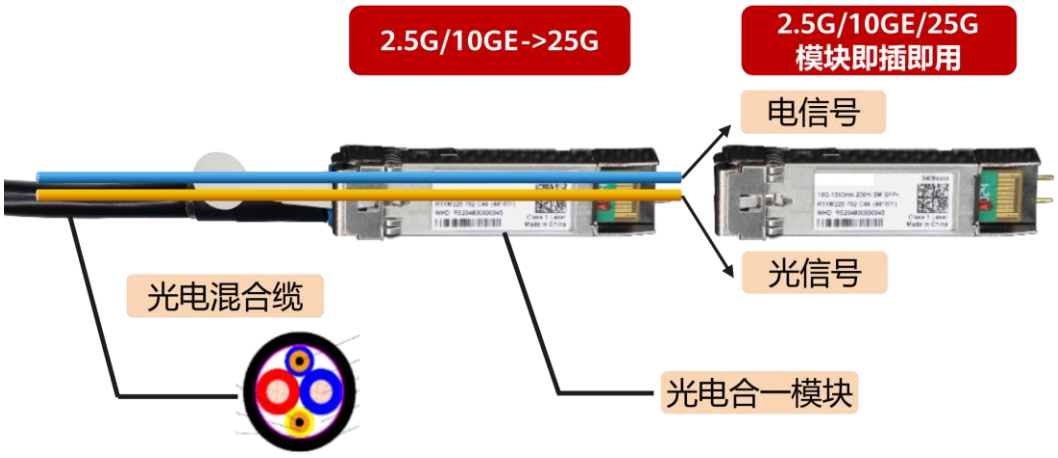
无源以太全光网络，兼具以太网协议和无源光网络架构优势：

- 极简架构：无源汇聚配套万兆接入的极简二层以太网组网架构，具备高密度可扩展的接入能力，可通过中心设备统一管理简化网络管理，同时无源汇聚免弱电间简化了部署要求。
- 统一标准：采用以太标准方案，继承了以太网超低时延、安全隔离等优势能力，又避免了协议转换导致的定位定界断点风险，无需企业运维人员学习多套技术体系。
- 万兆升级：融合 WDM&PON 优势，无源汇聚 160G 上行情况下，可实现 16 路独享 10G 全光入室。

有源以太全光网络，兼具全光纤介质组网和光电混合部署优势：

- 全光介质，弹性超宽：全网光纤介质，一次布线即可满足未来 10-15 年网络演进需求，特别的是满足未来超 10G 带宽演进，最大程度保护客户投资。
- 光电混合，远距 PoE（Power over Ethernet，以太网供电）取电：通过引入光电交换机和光电混合缆，提供了 PoE 技术在全光场景下持续演进的可能性，解决了网线 PoE 供电 100 米的限制，可实现终端超 300 米以上的远距 PoE 供电和网络覆盖的能力。

图4-4 光电混合缆示意图



以太全光方案适合房间密集、拉远部署等场景，无源以太全光方案和有源以太全光方案主要差异及相关建网方案选择建议参考表 4-1：

表4-1 以太全光方案选择建议

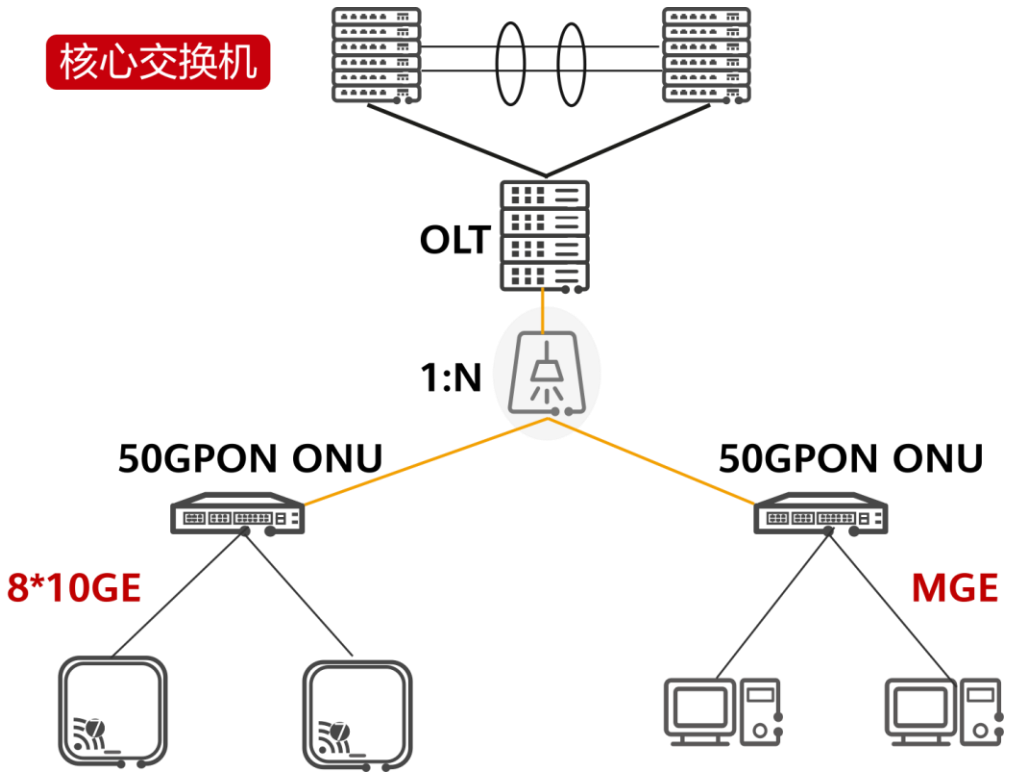
对比项	无源以太全光方案	有源以太全光方案
主用适用场景	末端终端数量经常变，比如教室，支持本地取电等类房间场景	终端数量基本固定，需要远程供电场景，独立办公室、无线办公，大开间场景。
末端设备位置	靠近终端，接近人的位置	弱电井，集中布置。
末端设备数量	8 口为主流	24&48 为主流。

对比项	无源以太全光方案	有源以太全光方案
介质	光纤到末端设备，末端设备通过短网线接终端	光纤到弱电井，弱电井出光电复合缆到房间/AP，或光纤到房间，末端设备通过短网线接终端。
优势	末端设备扩展灵活，扩容方便	设备集中管理，好维护，好施工，容易前提设计。
组网建议	• 无源汇聚选择 1U 支持 96*10G 端口以上高密设备，节约弱电机房空间 • 满足高品质业务承载和 WiFi-7 部署需求，建议选择 10GE/2.5GE 到 AP/终端组网	• 中心交换机可以为远端接入单元提供 300m 长距 PoE++供电，支撑远距网络覆盖能力 • 满足高品质业务承载和 WiFi-7 部署需求，建议选择 10GE/2.5GE 到 AP/终端组网

4.3 万兆 PON 光网

万兆 PON 光网支持超大带宽和确定性体验，共享 10G/50G 带宽，OLT 上联交换机实现接入企业骨干网络。

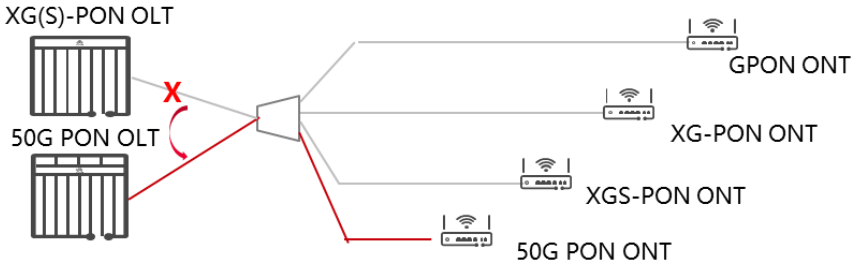
图4-5 万兆 PON 光网组网图



支持平滑升级演进，原有 PON 板下 ODN 整口直接无损割接到 50 GPON 端口。

- 三模合一方案兼容全网 GPON 及 XG(S)-PON 终端，无需外置合波

- 32dB 光功率预算对齐现网 Class C+光功率预算



波长和速率规划

- 50G PON 波长规划：

  ITU-T 定义 50G PON 下行波长范围 1340~1344nm（中心波长 1342nm），上行波长有三种选择：1260~1280nm，中心波长 1270nm；1284~1288nm，中心波长 1286nm；1290~1310nm，中心波长 1300nm。考虑到带宽效率，50G PON 上行锁定 1286nm，与 GPON、10G PON 波分共存。

- 50G PON 速率规划：

  ITU-T 定义 50G PON 下行 50Gbit/s，上行速率有 12.5G、25G、50Gbit/s 三种，实现中推荐采用 25G/50G。

4.4 关键指标

建议万兆有线网络应达成如表 4-2 所示指标。

表4-2 极简超宽架构关键指标

分类	指标项	推荐值	基础达标值
带宽	核心 400GE 组网	支持	不支持
	接入交换机上行 25GE，汇聚 25GE 下行 100GE 上行	支持	不支持
	接入盒子面板直出堆叠端口	250Gbps	80Gbps
可靠性	M-LAG 支持升级业务不中断	支持	不支持

5 高品质万兆园区建网方案

5.1 高品质万兆园区网络定义和架构

高品质万兆园区网络是具备万兆超宽、确定可靠、体验保障、智能运维、安全防护、绿色低碳能力的下一代园区网络。

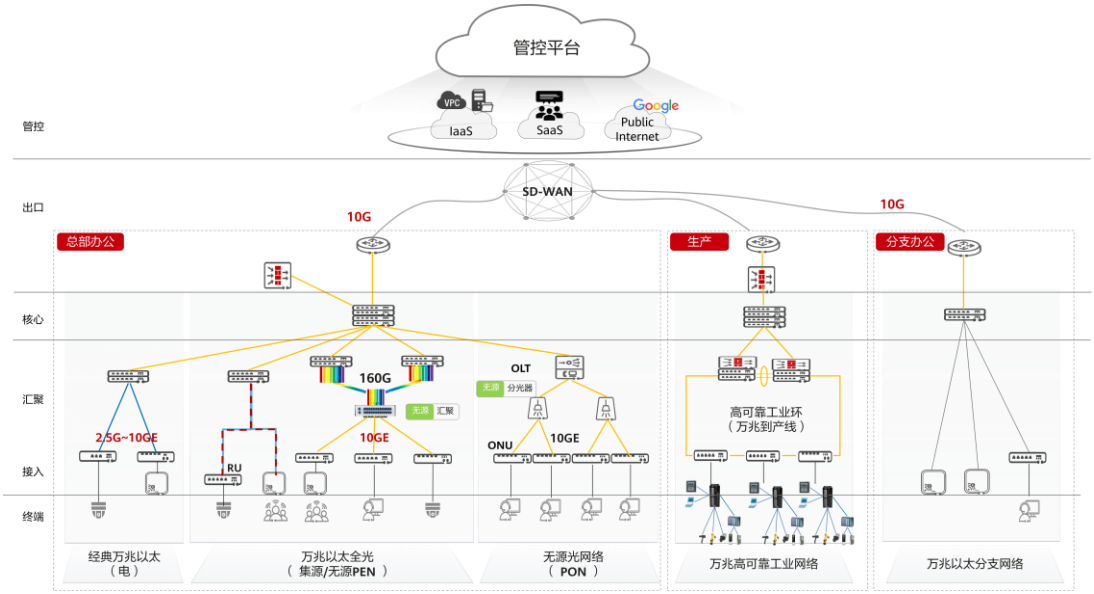
大部分万兆园区网是通过万兆以太网技术实现的。相比于千兆以太网，万兆以太网是采用以 Wi-Fi 7、2.5GE/10GE 交换机等以太网络设备为代表的园区网络，让企业和行业用户具备 10Gbps 接入速率带宽能力。

从网络架构看

如图 5-1 所示，万兆园区的承载网络设备包含园区出口设备、网络核心层设备、网络管理设备、接入层设备等。

- **终端层：**园区办公、生产等各种接入终端，包括智能终端、哑终端和工业终端等。
- **接入层：**接入终端的网络设备层，提供 2.5G~10G 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，充分体现了园区架构极简演进，支撑万兆接入能力，包括经典以太和以太全光两种主流方案，部分园区采用无源光网络方案。
- **核心层：**一般会对接防火墙、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。
- **出口层：**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。

图5-1 万兆园区网络架构图



从业务场景看

- **首先是万兆到办公。**万兆到办公是指办公室或者房间达到万兆。以教室举例，一个教室里有 10 到 13 个信息点位，每个信息点位动辄几百兆的流量，则教室里的总带宽需求也是达到了万兆。
- **其次是万兆到生产。**生产场景也需要万兆，如汽车产线这类需要用到高清工业 IPC（IP camera，网络摄像机）的场景，每路 IPC 2.5G 的带宽，则 1 条产线 4 台 IPC，即达到万兆带宽需求。
- **最后是万兆到分支。**高清视频每路带宽 160M，企业分支只要有 50 人并发，带宽需求就达到 8Gbps，业务全云化驱动分支带宽从千兆向万兆升级。

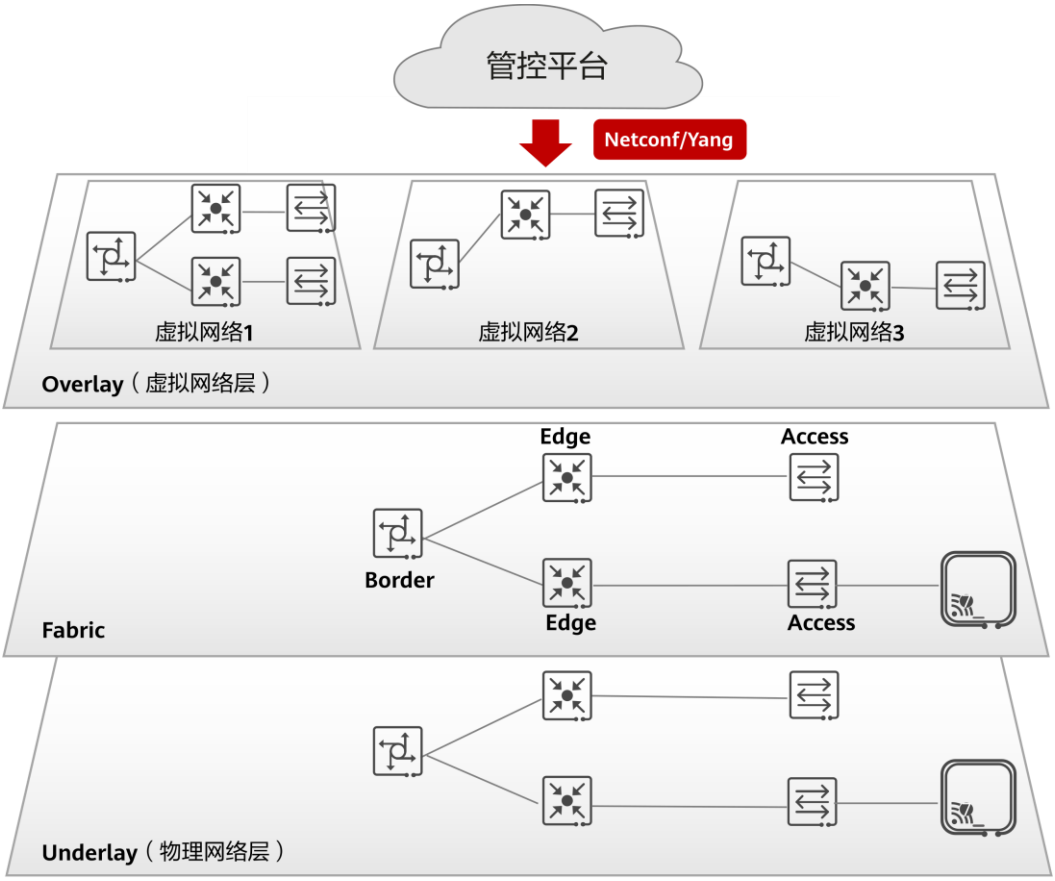
5.2 基于虚拟化技术实现 SDN 灵活网络架构

5.2.1 VXLAN 虚拟化方案

为了解决大中型园区网络极简部署和变更，支撑园区业务敏捷发放和快速演进，需要基于 SDN 网络控制器和 VXLAN（Virtual Extensible Local Area Network，虚拟扩展局域网）技术，实现网络资源池化和任意灵活调整。其主要技术和价值包括：

- 通过虚拟化技术，将物理网络资源池化，即在同一物理网络上虚拟出多个逻辑独立的虚拟网络，分别承载多种不同的业务。实现一网多用融合承载，及不同用户和业务的隔离。
- 采用 SDN 管控析平台实现网络和业务的自动配置发放，通过 Netconf、Telemetry 等技术实现对南向网络的管控。SDN 控制器可以实现对网络、设备、应用的抽象和解耦。
- VXLAN 是一种适用于园区虚拟化的网络协议标准，VXLAN 具备自动化部署、无状态的 VPN、L2、L3VPN 合一、可以穿越任意 IP 网络等优势，很好的解决了园区设备能力不一，改造难度大等问题。

图5-2 SDN 管控平台



虚拟园区网络层次及概念：

- 物理网络层（Underlay Network）：是由实体网络设备（如交换机、AP、防火墙、路由器等）建立的物理拓扑组网，为园区所有业务提供互联互通的能力，是园区业务数据转发的基础承载网络。
- Fabric：是通过虚拟化技术（VXLAN）构建在物理 Underlay 拓扑之上的全互联逻辑拓扑。业务网络在 Fabric 上创建，从而实现业务网络与物理网络的解耦，当业务网络需要调整变化时，不需要改变物理网络的拓扑结构。
- 虚拟网络层（Overlay Network）：是在物理层基础上通过虚拟化技术抽象出来的，将物理层网络资源进行池化处理，让业务层可按需调度的网络资源池。VN（Virtual Network，虚拟网络）是在 Fabric 上基于业务需求创建多个虚拟网络，实现业务隔离。例如，传统园区网络为了实现业务隔离，办公网和安防网是独立的两套物理网络，在虚拟化网络中，通过虚拟网络层实现物理网络的共享，通过创建两个 VN 即可实现在一套物理网上创建业务隔离的办公网和安防网。

5.2.2 SRv6 虚拟化方案

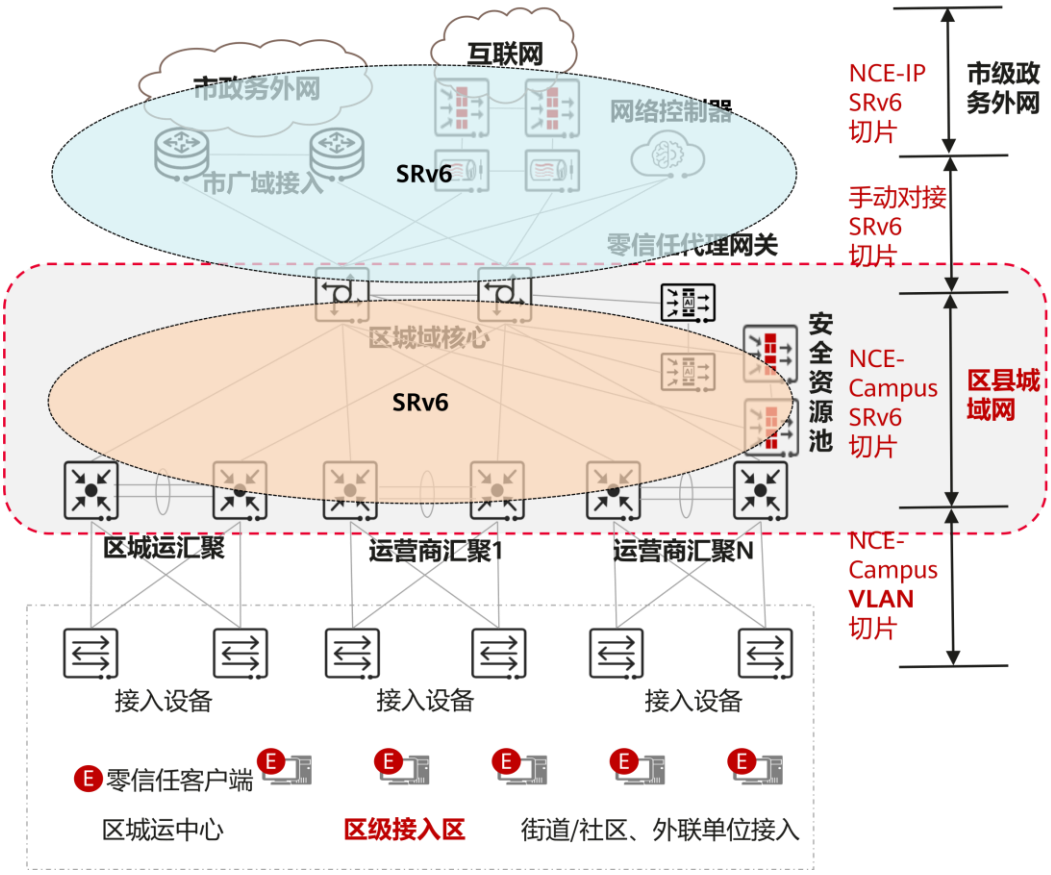
IPv6 能够提供海量的网络地址资源，是实现万物互联，促进生产生活数字化、网络化、智能化发展的关键要素。发展基于 IPv6 的下一代互联网，不仅是互联网演进升级的必然趋势，更是助力互联网与实体经济深度融合、支撑经济高质量发展的迫切需要，对于提升国家网络空间综合竞争力、加快网络强国建设具有重要意义。

SRv6（Segment Routing IPv6，基于 IPv6 转发平面的段路由）技术就是采用现有的 IPv6 转发技术，基于源路由理念而设计的在网络上转发 IPv6 数据包的一种协议。SRv6 通过在 IPv6 报文中插入一个路由扩展

头 SRH（Segment Routing Header），在 SRH 中压入一个显式的 IPv6 地址栈，并由中间节点不断的进行更新目的地址和偏移地址栈的操作来完成逐跳转发。SRv6 将一些 IPv6 地址定义成实例化的 SID（Segment ID），每个 SID 有着自己显式的作用和功能，通过不同的 SID 操作，实现简化的 VPN，以及灵活的路径规划。

SRv6 作为面向 IPv6+时代的关键协议标准，也具备了提供园区互联的能力，可适用于区县政务电子外网和教育城域网等场景。

图5-3 区县电子政务外网 SRv6 方案



方案特点

- **自动化部署：**SDN 极简部署、智能运维、主动安全
- **统一管理：**一套 SDN 平台，多区县统一集约化管理
- **大容量：**SDN 平台可纳管海量设备，无忧扩容
- **分权分域管理：**一套系统各区县分权分域管理，多租户安全隔离
- **架构开放：**北向 Restful 接口，方便二次开发或集成

5.2.3 关键指标

高品质万兆网络的 SDN 能力建议指标如表 5-1 所示。

表5-1 虚拟化关键指标

分类	指标项	推荐值	基础达标值
VXLAN 自动化	VXLAN Underlay 自动化	支持	支持
	VXLAN Overlay 自动化	支持	支持
LAN-WAN 融合	一套控制器同时管理 LAN-WAN 设备的同时，支持企业站点级设备即插即用，支持多站点快速批量复制	一套控制器同时管理 LAN-WAN 设备，实现站点级即插即用、AR 出口下挂交换机/AP 等设备免 ESN 开局，千站点天级完成批量复制	一套控制器同时管理 LAN-WAN 设备

5.3 基于确定可靠技术提升生产网络质量标准

传统的工业生产网络由于历史原因，一般都是基于业务系统进行建设。如城市管廊中会建设环境监控、消防和安防独立的物理网络；又如煤矿井下会建设安全监控环网、控制通信环网、视频监控环网等多张业务环网。基于业务系统建设网络的方式存在建设成本高、设备冗余和维护不便等明显问题。之所以采用这种方式，主要是受限于传统网络技术，无法在同一张网络上保障不同业务之间的 SLA。

确定性网络，是指利用确定性技术打造可预期、可规划、可验证，有确定性能力的专用网络，提供差异化的业务体验。行业应用的需求千差万别，差异化网络是生产数字化的关键诉求。比如远程抄表，需要的网络联接很多，对带宽和时延并不敏感；而远自动驾驶等业务对网络的确定性低时延、安全可靠要求很高。专属网络资源保证数据安全隔离、保护数据隐私，是行业应用的普遍要求。

当前确定性技术主要有 TSN（Time Sensitive Networking，时间敏感网络）和网络切片两种，TSN 能够提供超低时延以及时钟同步等能力，同时也由于 TSN 生态范围有限，故主要在生产 OT（Operation Technology，操作技术）网使用，重点应用在 PLC（Programmable Logic Controller，可编程逻辑控制器）和 I/O（Input/Output，输入/输出）之间的网络组网；网络切片从逻辑资源上保障了业务的 SLA，更适合在生产 IT（Information Technology，信息技术）网使用，在提供一张业务融合网络的同时，还具备各自业务的 SLA 诉求。

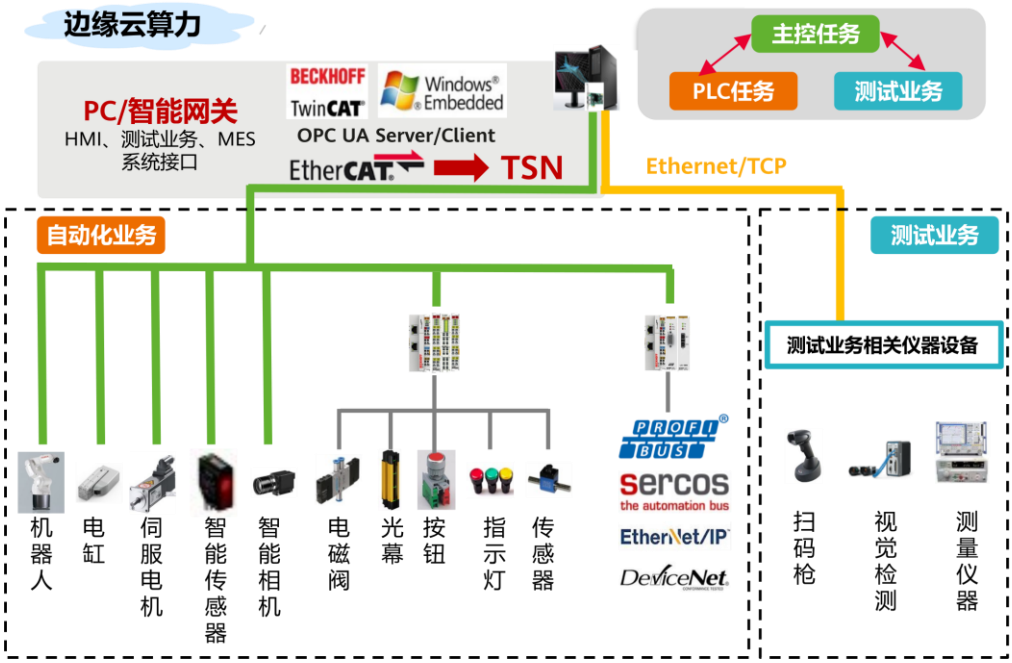
5.3.1 TSN

TSN 是 IEEE802.1 任务组基于以太技术开发的一套数据链路层协议规范，在以太网传输机制中引入时间敏感机制，为数据链路层提供更可靠的、低延迟、低抖动的数据传输服务。

传统以太网络中，突发流量和冲突是引起抖动、丢包和时延不能保障的根本原因，为解决传统以太网络的问题，TSN 引入了新的机制：1）预留缓存和带宽资源，规避冲突；2）使用队列和调度规则控制冲突，使得突发流量和冲突的行为可预测；3）转发调度增强，保障调度时延及抖动；基于高精度时钟同步，提供精准调度；4）帧抢占机制，保障 TSN 流及时被调度；5）冗余路径，提供高可靠传输。

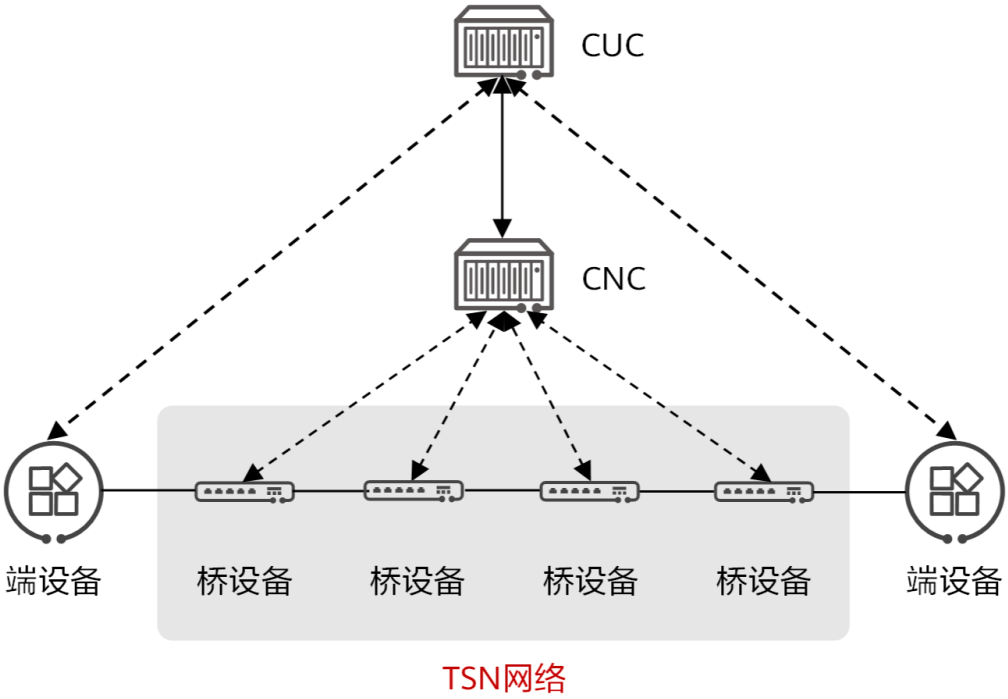
通过上述机制，实现零拥塞丢包的传输，提供有上界保证的低时延和抖动，为时延敏感流量提供确定性传输保证，可为生产网集中化和云化改造场景提供稳定可用的承载网络。

图5-4 PLC 集中部署场景



TSN 网络的功能架构遵循 SDN 技术思路，并按照 IEEE 802.1Qcc 协议要求，将整个系统分为控制管理单元（包括 CNC（Centralized Network Configuration，集中网络控制）和 CUC（Centralized User Configuration，集中用户配置））、传输单元（网关、交换机）、应用单元（工业端设备、基站等）三种功能单元，如图所示。

图5-5 TSN 网络功能架构



- **管理单元：**CUC 负责用户对网络需求的翻译及网络信息和设备配置的域间协同，CNC 在同一个 TSN 网络域内负责实现设备监控管理、网络拓扑发现、流量监控及调优，业务建模及调度模型下发等功能。
- **传输单元：**除了支持 TSN 网络相关转发特性，还支持相关在线测量协议，实时将相关状态上送给管理单元，从而实现全网实时监控，根据网络需求和状态，动态调整相关配置。
- **应用单元：**具备接入 TSN 网络的能力，支持在线测量及运行维护相关协议，以实现全网拓扑发现、状态监测以及网络业务调优。

5.3.2 网络切片

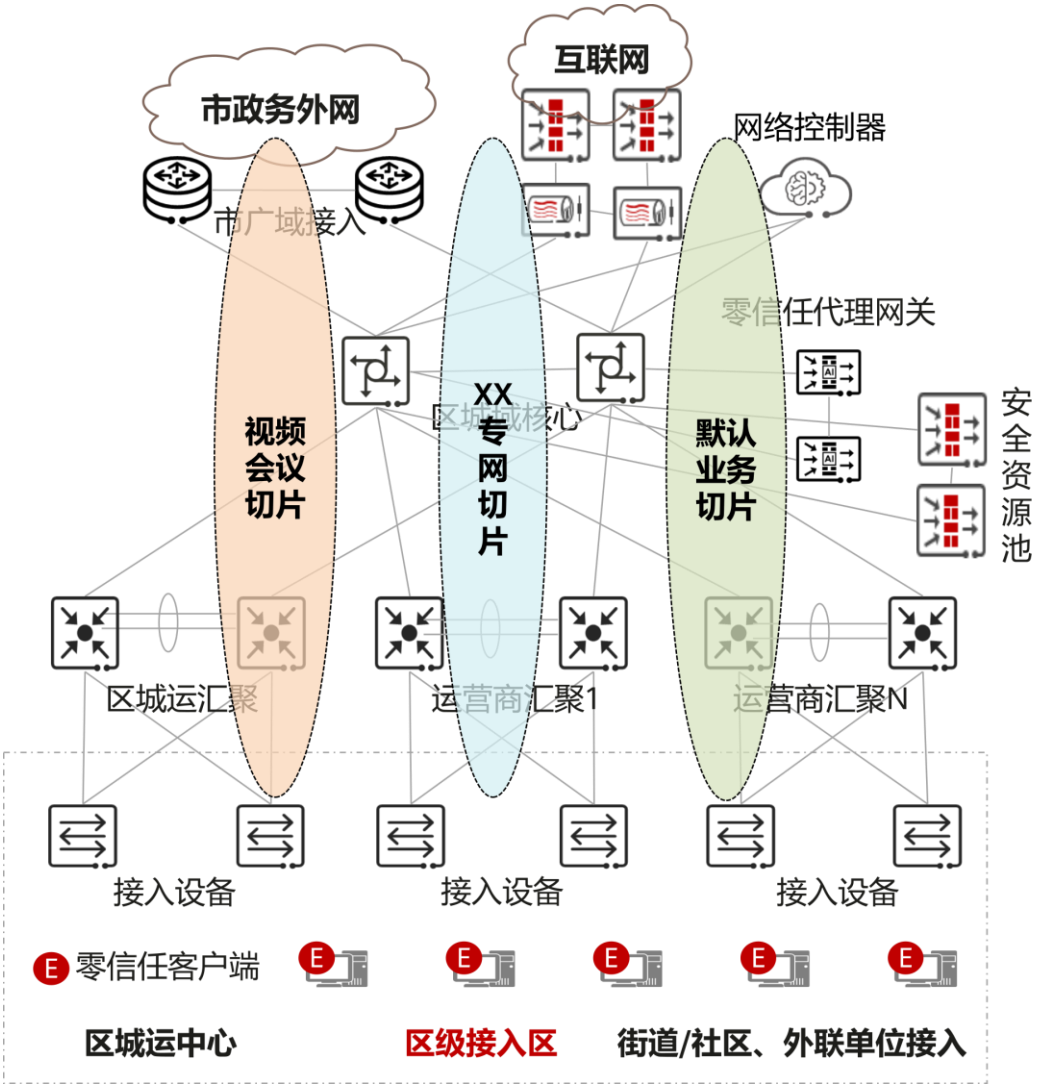
网络切片是通过网络资源预留的方式，实现业务隔离的一种网络虚拟化技术，包括 FlexE 接口、信道化子接口和 Flex-channel 等方案。

网络切片相当于设备为每个网络切片划分独立“车道”，不同网络切片的“车道”之间是实线，业务流量在传输过程中不能并线变换“车道”，从而确保不同切片的业务在设备内可以严格隔离，有效避免流量突发时切片业务之间的资源抢占。

网络切片通过在同一个共享的网络基础设施上提供多个逻辑网络（切片），使每个逻辑网络服务于特定的业务类型，资源预留技术是网络切片提供差异化 SLA 保障的关键。资源预留技术将物理网络中的转发资源划分为相互隔离的多份资源，分别提供给不同的网络切片使用，保证网络切片内有满足业务需求的可用资源，同时避免或者控制不同网络切片之间的资源竞争与抢占。

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，以满足不同业务的差异化需求，从而根据业务需求进行资源预留。通过构筑端到端切片网络，可以实现不同业务统一承载，并对不同业务进行精细化管理，切片需要支持基于 SRv6/VXLAN 组网、VLAN 组网以及 SRv6/VXLAN+VLAN 混合组网，以实现端到端业务保障能力。

图5-6 市-区县切片解决方案



5.3.3 可靠性

网络可靠性是网络在发生故障或遭遇攻击的情况下，仍能正常工作并为用户提供满意的服务的能力。可靠性包括设备可靠性和组网可靠性，重要节点的设备应在网络设计上考虑冗余和备份，减少单点故障对整个网络的影响。

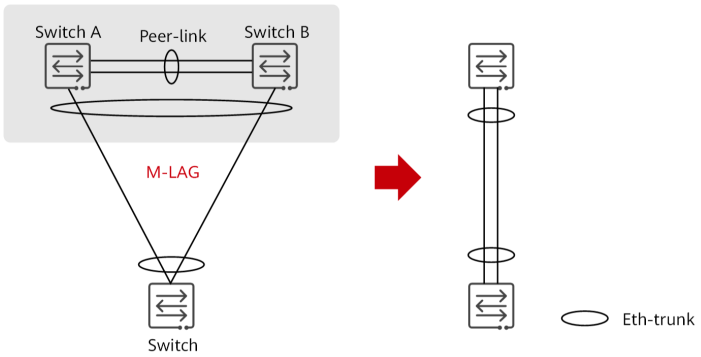
网络冗余技术

网络冗余技术主要包括 M-LAG（Multichassis Link Aggregation Group，跨设备链路聚合组）技术和堆叠技术。M-LAG 技术通过将两台设备虚拟成一台设备，实现设备的冗余，但实际架构中还是独立的两个控制面，这样可以实现单台设备的独立升级；堆叠技术是将 2 台及以上的设备组成一个堆叠组，实现了端口的扩展，堆叠组只有一个控制大脑，体现为一台设备。

- M-LAG：一种实现跨设备链路聚合的机制，图 5-7 将 Switch A 和 Switch B 通过 Peer-link 链路连接并以同一个状态和 Switch 进行链路聚合协商，从而把链路可靠性从单板级提高到了设备级。当某条

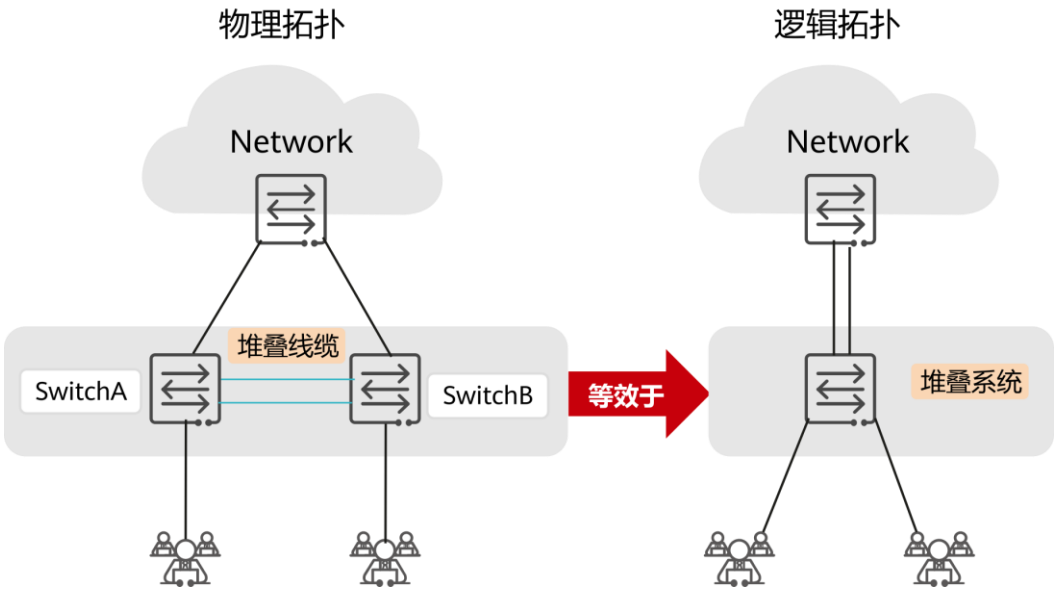
上行链路、下行链路、Peer-link 链路或心跳链路故障时，以及单台 M-LAG 交换机故障时，M-LAG 均可自行完成流量的切换。

图5-7 M-LAG 示意图



- 堆叠技术：一种将多台支持堆叠特性的交换机通过堆叠线缆连接在一起，从逻辑上虚拟成一台交换设备的技术。作为园区虚拟化和可靠性的关键技术，堆叠特性是园区必备的基础特性，可通过多台设备虚拟化成一台设备，简化组网减少管理代价，同时双上行和本地转发提升了转发性能、端口容量和可靠性能力。

图5-8 堆叠示意图

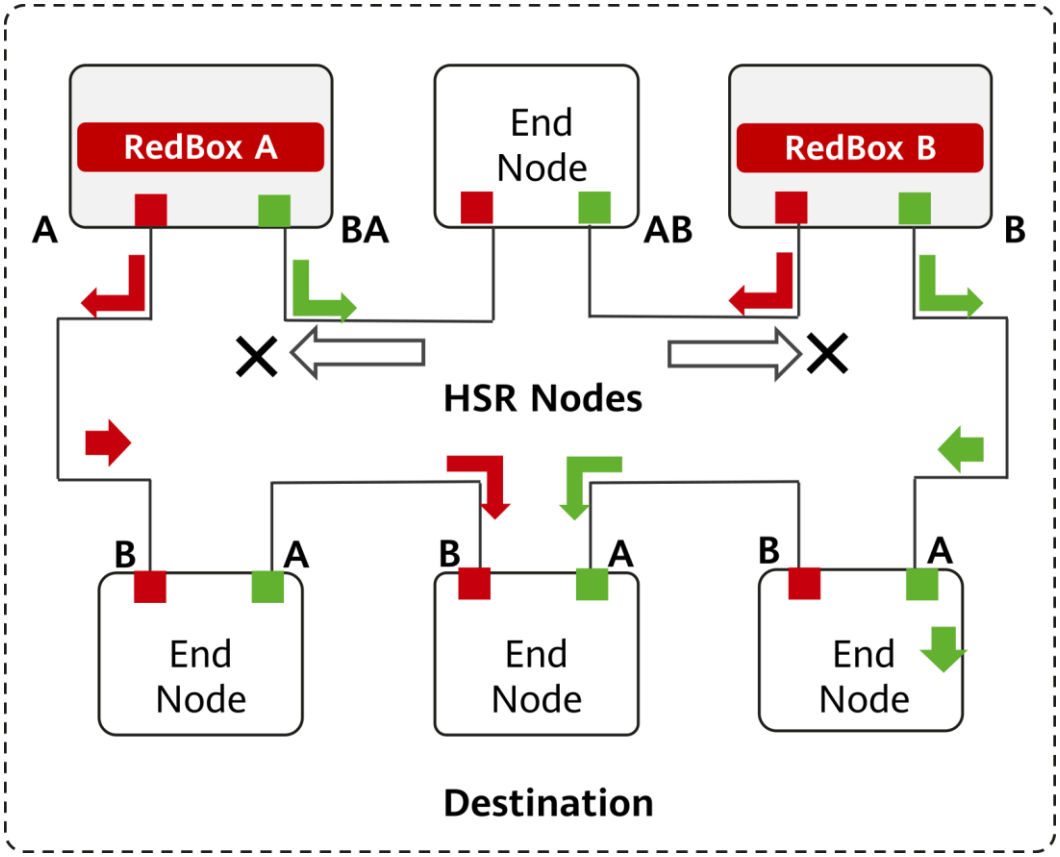


快速检测技术

协议可靠性则是通过快速检测技术，感知到故障点后完成业务路径的快速切换，包括传统的 OSPF（Open Shortest Path First，开放式最短路径优先）、BGP（Border Gateway Protocol，边界网关协议）等三层检测技术，也包括 HSR（High-availability Seamless Redundancy，高可靠性无缝冗余）、ERPS（Ethernet Ring Protection Switching，以太网环保护）等二层检测技术，在生产 OT 网络中二层技术的应用更为广泛。

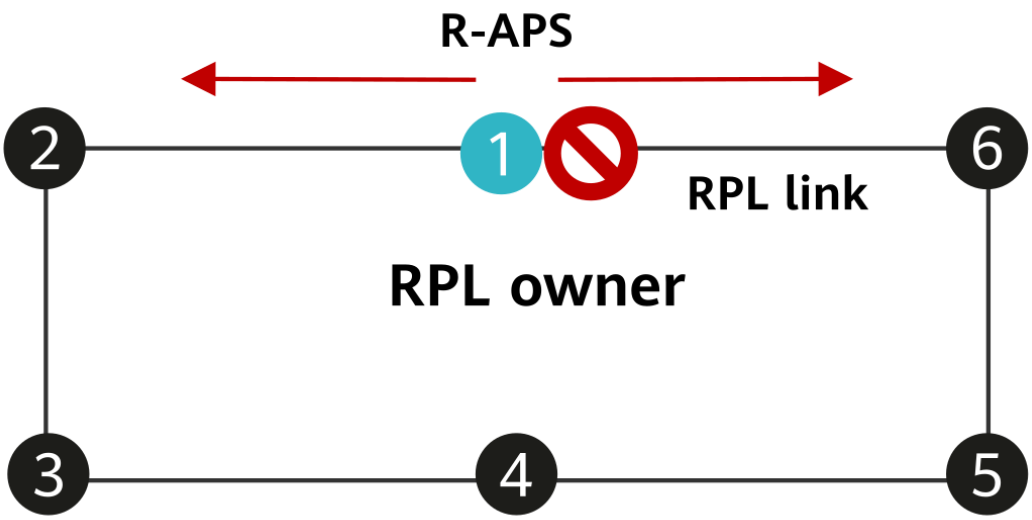
- HSR：一种基于以太网的二层冗余协议。HSR 是 IEC62439-3 中定义的国际标准，主要应用于变电站以及运动控制等对可靠性具有严苛要求的场景。通过在源节点插入 HSR 标签并向环网双端口同时转发流量，目的节点选收，从而实现双发选收高可靠性。其原理为：在 RedBox（Redundancy Box）A 发送从其上层收到的帧，在其前面加上 HSR 标记以识别帧重复，并通过每个端口发送帧（“A”帧和“B”帧）。目的节点 End Node 在特定时间间隔内从每个端口接收两个相同的帧，转发第一帧，删除该帧的 HSR 标记，并丢弃之后收到的任何重复帧，其技术原理如图 5-9。

图5-9 借用环网的双向路径构建网络的可靠性能力



- ERPS：ITU-T 定义的一种二层破环协议标准，用于在以太网层面进行环网拓扑的保护倒换。它以 ERPS 环为基本单位，包含若干个节点，通过阻塞 RPL Owner 端口，并控制其他普通端口，使得端口的状态在 Forwarding 和 Discarding 之间切换，达到消除环路的目的。如图 5-10 所示，ERPS 环网指定一条链路为 RPL（Ring Protection Link，环路保护链路），与之相连的一个节点称为 RPL Owner。在正常状态下，RPL Owner 阻塞其 RPL 端口以防止业务形成环路，并定时向以太网环上发送 R-APS 消息。一个环只有一条 RPL 和一个 RPL Owner，当有多个 RPL Owner 存在时，系统会上报相应的告警。

图5-10 ERPS 环网状态



5.3.4 关键指标

高品质生产网络的建议指标如表 5-2 所示。

表5-2 确定性关键指标

分类	指标项	推荐值	基础达标值
确定性	TSN 支持万兆口	支持	不支持
	1588v2 时钟精度	30ns	50ns
	除了常规的 8 个 QOS 队列外还可以为业务分配独享的带宽资源，确保业务服务质量	支持	不支持
可靠性	ERPS 环网高性能切换(标准 ERPS 协议并支持与三方对接)	20ms	50ms

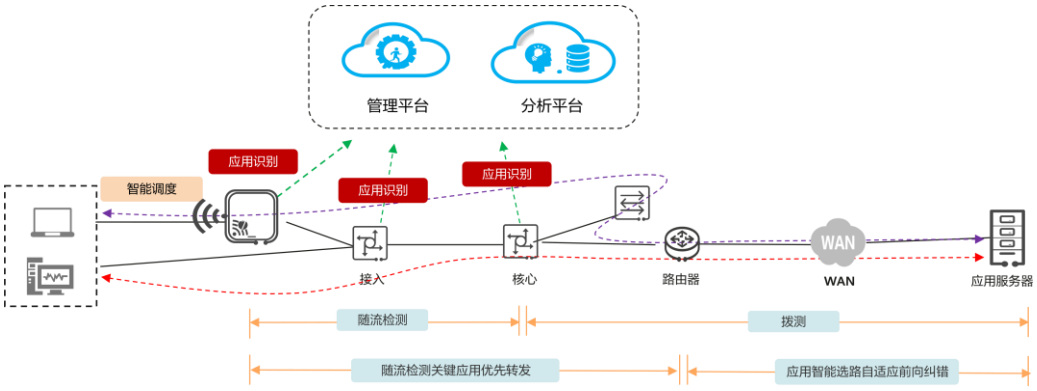
5.4 基于体验保障构建高品质网络

基于应用识别、多媒体智能调度、应用智能选路和随流检测等技术，构建应用路径可视、关键应用可保障、应用问题可定界的高品质网络。通过 VIP 优先接入和 VIP 带宽预留技术保障在高密接入场景下 VIP 用户的访问体验。

5.4.1 应用保障

针对应用路径不可视、转发优先级无保障、出现问题难定位问题，基于应用识别、多媒体智能调度、应用智能选路、自适应前向纠错和随流检测等技术，构建应用路径可视、关键应用可保障、应用问题可定界的高品质网络。

图5-11 应用保障网络架构



应用识别

传统流量分类技术只能检测 IP 报文的 4 层以下的内容，包括源地址、目的地址、源端口、目的端口以及业务类型等，而无法分析出报文的应用。应用识别在分析报文头的基础上，对报文中的第 4～7 层内容和一些协议(如 HTTP、FTP)进行检测和识别，是一种基于应用层的流量检测。常见的识别方式如下：

- 基于协议端口的应用识别
- 基于签名的应用识别
- 基于协议关联的应用识别
- 基于行为分析的应用识别
- 多维度组合的应用识别

关键应用优先转发

在应用识别的基础，将关键应用报文的 QoS 优先级修改成高优先级，从而保障关键应用报文在整个网络中优先转发，同时降低转发时延，在网络中有大流量时确保 RTT<100ms。

Wi-Fi 多媒体智能调度

在 Wi-Fi 技术中，传统 QoS 是通过 EDCA（Enhanced Distributed Channel Access，增强型分布式信道访问）竞争参数控制的，主要逻辑是对不同业务配置不同的随机回退参数，调整其空口抢占能力，实现不同业务的差异化调度能力，但是存在不同业务抢占空口导致应用质量变差的问题。比如，在存在大文件上传下载的业务，会抢占同时进行的多媒体业务(语音/视频)的发送机会，导致其体验变差。多媒体智能调度算法通过应用识别技术来区分高优先级多媒体业务和低优先级“贪婪业务”（持续时间长的大带宽业务），再对多媒体业务的业务时延进行监测，发现这些业务受损时，通过拥塞控制算法抑制“贪婪业务”流量，让用户享受高速网络的同时，语音视频业务也不受影响。通过基于拥塞控制的多媒体业务保障算法，可以在网络出现因为“贪婪业务”而拥塞的情况下，精准抑制和调度，让关键的多媒体业务时延有边界。

应用智能选路

分支互连网络提供最优路径动态选择、逐流/逐包负载分担、多发选收等多种选路算法。基于业务随流检测技术，能够精准感知应用 SLA，当网络 SLA 不满足应用要求时，能够秒级实现主备路径切换。可以根据应用诉求进行智能选路，即能够实时监控网络的质量，并根据应用对 SLA 质量诉求，在多条不同网络质量的 WAN 链路上，动态、自动地选择符合应用 SLA 质量要求的网络路径，同时兼顾 WAN 网络的整体使用效率，称之为智能选路。支持多种智能选路策略，包括链路质量选路、负载均衡选路、应用优先级选路、带宽利用率选路。

自适应前向纠错

能够根据网络丢包情况，自适应调整冗余包，避免网络丢包较少时过多的冗余包消耗链路带宽。FEC（Forward Error Correction，前向纠错）通过流分类拦截指定数据流，增加携带校验信息的冗余包，并在接收端进行校验。如果网络中出现了丢包或者报文损伤，则通过冗余包还原报文。设备自动检测网络丢包率，根据丢包率实时调整冗余包的数量。该方式可以在丢包少的时候减少冗余包，节约带宽；在丢包率变高时增加冗余包，提升抗丢包能力。通过 A-FEC（Adaptive Forward Error Correction，自适应前向纠错）保障链路丢包 30%视频不卡顿。

多发选收

发送端 CPE 对数据包进行复制，把原始包和复制包通过多条链路中的两条一起发送。如果一条链路上有丢包，则接收端 CPE 通过另一条链路上的冗余包还原，从而不用重传。多发选收适用于流量小、高可靠的业务。例如：VoIP、付款业务、5G 工业场景（工业机器的 PLC 控制信息对时延要求极高，不能接受重传）。

智能策略推荐

快速识别全网中的 TOP 拥塞站点，并自动生成应对策略、有效解决网络中的拥塞点，实现网络级全局最优负载均衡。基于大数据分析的带宽推荐，提供未来 12 个月的带宽预测，帮助客户精准进行广域链路带宽扩容，彻底解决链路带宽扩容缺乏依据完全依赖人工经验的问题。与此同时，能够提供现网流量数据的历史回放，让园区外网络带宽占用一目了然。

SaaS 智能选路

支持通过在不同路径下模拟 SaaS 应用访问，获得该路径下的真实业务体验数据，通过不同路径下的体验数据对比，最终为 SaaS 优选一条最优的访问路径。

随流体验测量

传统的运维手段针对可复现的故障通过 Ping/Tracert 进行故障定界，并通过分析日志、流监控等信息进行故障定位，但针对不可复现故障（例如音视频短暂劣化）常常束手无策。随流体验测量技术可以针对音视频会议流量进行全流监控，检测音视频会议每条流的丢包和时延，如果出现音视频劣化的问题，可以通过分析历史记录进行逐跳的故障定界定位，无需故障复现，体验类问题 5 分钟定界，从而大幅提升运维效率和客户满意度。

5.4.2 用户/终端保障

针对无线网络体验不佳问题，通过 VIP 优先接入和 VIP 带宽预留技术保障在高密、弱覆盖、拥塞、快速移动场景下 VIP 用户的访问体验。网络规划时，把企业关键用户规划为 VIP 用户，针对 VIP 用户建议部署 VIP 用户优先接入和 VIP 用户带宽预留。

用户优先接入

VIP 用户优先接入是当接入用户数达到 AP 最大用户数或用户数量门限时，如果再有新用户接入到网络，该用户先进行认证，认证成功后，在授权阶段判断该用户是否是 VIP 用户，如果是，则允许该用户接入并替换一个非 VIP 用户，强制该非 VIP 用户下线；如果不是，则强制该用户下线，从而保障 VIP 用户的优先接入。

用户带宽预留

VIP 用户空口带宽预留算法基于射频，通过为 VIP 用户预留相应的时间切片保证 VIP 用户的体验。预留的带宽由所有 VIP 用户共享。

优先转发

使用带宽预留的方案仅能保障下行拥塞的场景，如果出现上行拥塞场景是无法保障的，终端不遵从标准 EDCA，拥塞场景下，空口资源被贪婪终端抢占，影响 VIP 体验。此时需要采用 VIP 超帧抢占的方案。

VIP 超帧抢占可以针对 VIP 预留时间片（包含上下行）来实现 VIP 保障，在信道利用率 80%情况下保障 VIP 用户的 RTT < 50ms。如果无 VIP 用户和 VIP 无流量的场景则不会进行时间片预留。

5.4.3 关键指标

园区网络部署体验保障功能后，建议体验保障指标如表 5-3 所示。

表5-3 体验保障关键指标

分类	指标项	推荐值	基础达标值
应用保障	网络拥塞时大流量业务导致音视频会议卡顿，交换机/WLAN 的应用识别出 SaaS 类音视频会议，有线或无线接入，园区从核心到接入上下行端到端保障音视频会议不丢包。	支持上行和下行端到端保障	支持下行端到端保障
	音视频会议的应用识别和保障支持的终端数和带宽	3W 终端，600Gbps（背景+音视频会议流量）	5K 终端，100Gbps（背景+音视频会议流量）
	音视频体验差的时候能够抑制其他低优先级大流量业务保障音视频会议体验	支持同频 AP 的大流量抑制	支持 AP 内的业务抑制
	单 AP（40MHZ 组网）4K 音视频（码率 25Mbps）并发无卡顿	并发 10 路	并发 8 路
	单 AP（80MHZ 组网）4K 音视频（码率 25Mbps）并发无卡顿	并发 20 路	并发 16 路
	单 AP（40MHZ 组网）1K 音视频（码率 4Mbps）并发无卡顿	并发 50 路	并发 40 路
	单 AP（80MHZ 组网）1K 音视频（码率 4Mbps）并发无卡顿	并发 70 路	并发 60 路
	总部多分支互联园区，总部根据分支广域链路的实际可用带宽动态进行 QOS 限速	动态自适应调整 QoS	静态 QoS

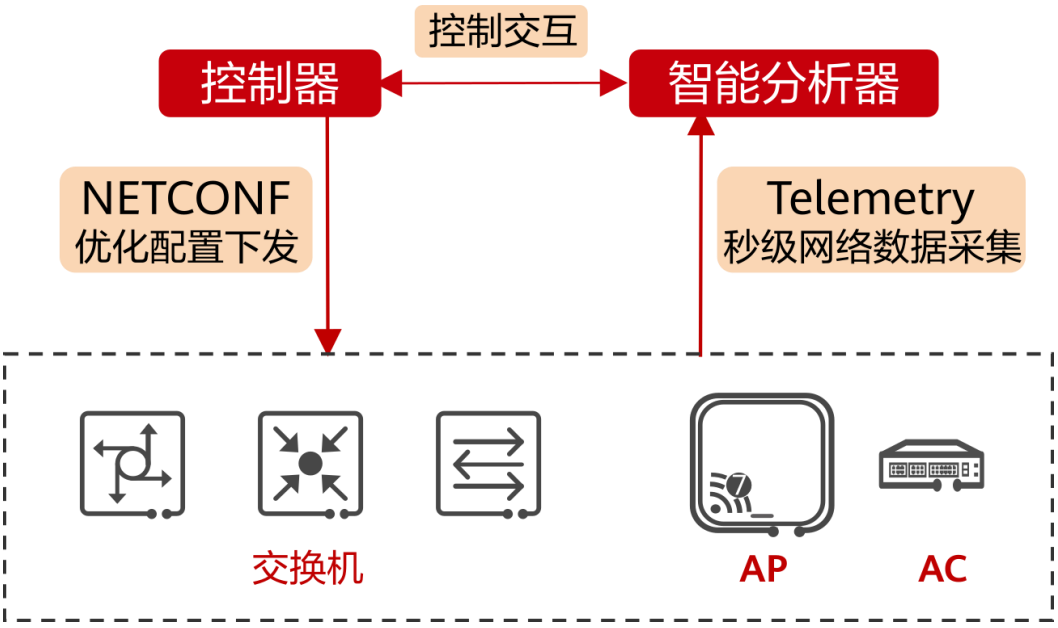
分类	指标项	推荐值	基础达标值
	自适应前向纠错技术，保障 30%网络丢包音视频不卡顿。	30%丢包不卡顿	20%丢包不卡顿
VIP 保障	空口 UDP 或 TCP 流量上下行拥塞导致空口信道利用率大于 80%的情况下保障 VIP 空口时延	50ms	200ms
	用户数达到 AP 上限的时候 VIP 优先接入	支持	不支持

5.5 基于 AI 和大数据构建智能运维网络

5.5.1 智能运维系统

智能运维系统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，通过数字地图方式来清晰呈现网络基础信息，实现全网一图可视，协助运维人员定位问题。智能运维工具包含控制器和智能分析器两部分，控制器实现配置下发，分析器实现数据收集、汇总和分析。

图5-12 智能运维系统架构图



部署自动化

ZTP（Zero Touch Provisioning，零配置部署）开局：设备支持 ZTP，具备邮件开局、U 盘、及 DHCP Option 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。

自动化部署：应具备 VXLAN 虚拟化的 Underlay 和 Overlay 的端到端自动化部署能力。

模板化定制：具备灵活的业务配置模板能力，多模板定制能力，以适应不同的园区站点；同时多个模板间具备灵活的组合、继承能力，提供的配置模板具备变参能力，以能够灵活部署不同站点或者设备的差异性网络业务，降低复杂度。

网络可视化

支持一张图呈现整个网络拓扑，打通网络、应用、用户/终端之间的关系，解决看不到、看不全、看不准的问题。类比交通地图，网络数字地图是物理网络世界的数字孪生，可视、可交互，构建数字化智能管理平台。

图5-13 网站数字地图

实时感知设备状态，通过 Telemetry 等技术精准采集设备信息，秒级感知设备异常，智能分析问题根因，同时可智能化提供处理建议。让机器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。

无线网络：基于 Telemetry 技术，监控无线侧关键指标。主动识别弱信号覆盖、高干扰、高信道利用率等空口性能类问题。

有线网络：基于 Telemetry 技术采集设备、接口、光链路等性能 Metrics 数据，主动监控、预测网络异常。使用 AI 算法对设备 CPU/内存利用率等指标进行基线预测。通过和动态基线的对比，在业务中断前识别网络指标的劣化。

定位智能化

智能分析：在问题发生时，智能网管工具应能基于采集信息，通过预置的故障知识库，自动快速给出根因分析，协助运维人员快速定界并解决问题，减少运维人员到现场定位问题的次数。

问题回放：在问题发生后，智能运维工具需要具备回放问题发生过程的能力，减少运维人员在处理已发生问题时到现场复现问题的次数，提高运维效率，降低运维成本。

预测性优化

智能运维工具需要支持收集和分析大量网络数据，通过机器学习算法，持续学习并适应网络环境的变化，通过预测性算法，提前预测问题，并启动自动化流程进行响应，快速纠正问题，降低网络问题发生的可能性。

LAN&WAN 融合

SD-WAN 通过集中化的网络运维和管理工具、完善的网络策略配置工具，实现 LAN&WAN 网络的统一管理，实现从网络开通、业务部署、故障定位、日常巡检全流程自动化。

5.5.2 关键指标

园区中部署智能运维系统后，建议网络运维达到如表 5-4 所示能力。

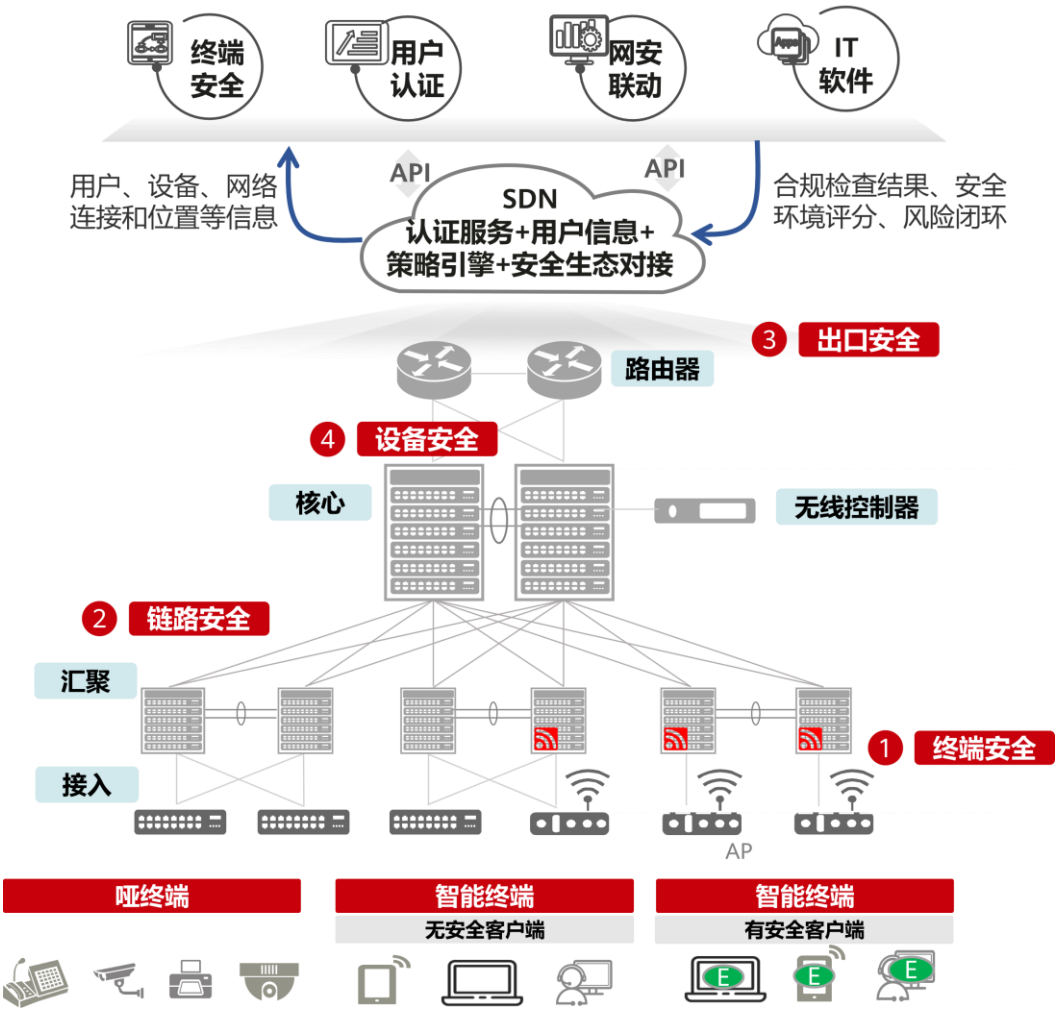
表5-4 智能运维关键指标

分类	指标项	推荐值	基础达标值
运维	有线健康度评估，支持如下能力进行统计和评估： 设备容量：比如 ARP 表项、MAC 表项、存储器容量 网络状态：比如端口闪断、光模块异常、端口假死 网络性能：比如端口拥塞、队列拥塞、端口误包 网络协议：比如 BGP 震荡，OSPF 震荡等	支持	支持
	无线健康度评估，包含如下问题的诊断： 支持度量 AP 上的用户接入成功率、用户接入耗时、漫游达标率、容量占用率、吞吐达标率	支持	支持
	数字地图支持网络、应用、用户、终端，多维可视，一图可视	支持一图可视	支持多图呈现
	基于自然语言的交互式运维，查询网络、用户、应用、能耗指标；网络、用户、应用的排障	支持	不支持
	支持针对园区内音视频媒体流量的丢包和时延进行实时监控，出现体验问题可以通过历史记录进行逐跳定界,空口+有线的丢包和时延测量精度 > 90%	同时监控 1000 个终端的音视频流 备注：每个终端上下行的音视频流总和为 20 个	同时监控 5 个终端的音视频流 备注：每个终端上下行的音视频流总和为 20 个
	基于数字地图实现空口、有线、广域端到端的丢包时延的完整测量和分段故障定界	端到端完整支持	分段支持
调优	射频功率、信道、频宽、粘性终端踢除，支持准实时优化	10 分钟	24 小时

5.6 基于零信任理念构建园区安全网络

零信任是一种网络安全模型，它基于“永不信任，始终验证”的原则，强调对所有用户进行持续验证和动态授权。基于零信任理念的园区网络安全解决方案需从终端安全、链路安全、出口安全和设备安全四个方面需要提供全方位安全防护。

图5-14 园区网络安全架构



5.6.1 终端安全

通过终端识别技术，实现园区内的终端可视，并基于终端类型可免认证接入网络、分配不同的网络权限。在终端识别的基础上，通过监测同一 MAC 的终端类型是否变化，实现防仿冒的功能。通过监测设备端口上的终端流量特征，实现防仿冒和防私接功能。

终端识别

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和主动扫描两大类。

- 被动指纹采集：通过交换机采集终端报文中的 MAC OUI、HTTP UserAgent、DHCP Option、LLDP 等特征指纹，上报给园区网络管理系统，然后通过匹配园区网络管理系统自带的指纹库进行终端类型识别。当存在未知终端时，可通过 AI 算法自动提取终端指纹或自定义指纹存到指纹库，提高终端识别率。
- 主动扫描：对于网络中的静默终端，由于其低频次通信的特点，难以通过被动指纹识别方式感知终端类型，为了更高效的发现设备，终端识别引擎发送 ONVIF 等探测报文，从回应报文中获取终端类型、型号、厂商等信息。

终端防仿冒

终端仿冒检测是指通过识别接入园区网络的终端流量是否符合相应类型终端的流量行为模型，从而判断终端是否异常的技术。流量行为模型是终端访问园区网络的流量特征，如访问的 IP 集合、TCP/UDP 端口集合、TCP 连接个数等。

终端防私接

通过部署检测组件到园区接入网络设备，检测组件被动上送终端设备发送的报文，交换机基于终端报文提取出报文特征并根据识别规则解析出终端画像特征后检测其是否跳变，如存在跳变则判断存在私接终端，保存结果检测到私接类型并反馈结果至 SDN 控制器。

5.6.2 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，通过 IPsec 实现 IP 数据报文加密。

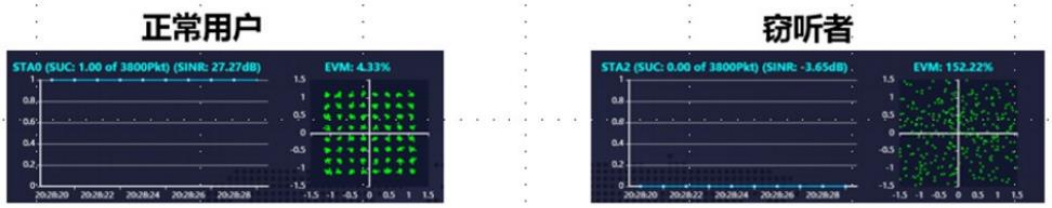
WPA

WPA（Wi-Fi Protected Access，Wi-Fi 保护访问）有 WPA、WPA2 和 WPA3 三个标准，是一种保护无线网络安全的系统。支持 EAP-PEAP、EAP-TLS 等认证方式。

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，如图 5-15 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5-15 不同用户收到的信号图

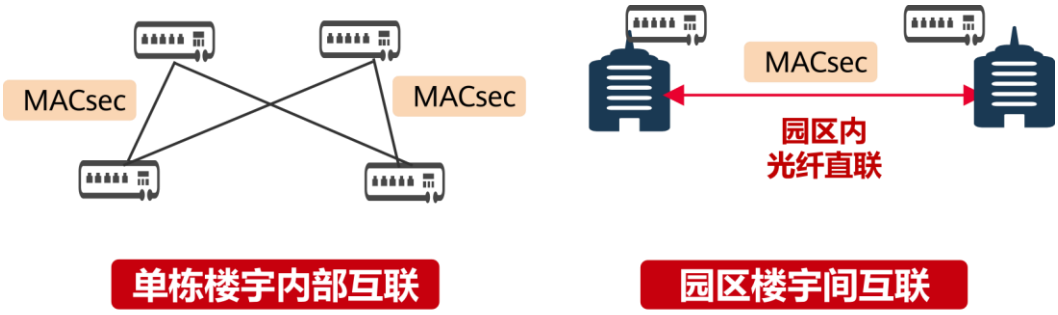


考虑到全无线移动办公的普及，空口加扰需要能在终端移动位置后，快速更新信息，保证空口加扰准确性。

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，在单栋楼宇内部互联和楼宇间光纤互联部分部署。

图5-16 MACsec 部署位置图



IPsec

IPsec 是 IETF 制定的一组开放的网络安全协议。它并不是一个单独的协议，而是一系列为 IP 网络提供安全性的协议和服务的集合，包括 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷协议）两个安全协议、密钥交换和用于验证及加密的一些算法等。

5.6.3 出口安全

通过防火墙、安全沙箱和安全态势来构建出口安全网络。

防火墙

边界防火墙进行流量访问控制，同时防火墙集成 IPS（Intrusion Prevention System，入侵防御系统）、AV（Antivirus，防病毒）等安全防御能力，可以对网络攻击进行检测。防火墙也可按需开启 NAT(Network Address Translation，网络地址转换)、IPsec 等能力。

安全沙箱

针对未知的文件检测，防火墙可联动沙箱进行安全检测，沙箱通过模拟恶意文件的运行，基于行为发现未知恶意文件，并且和防火墙形成联动，通过防火墙阻断恶意文件入侵。

安全态势感知/流探针

流探针设备采集核心交换机流量，并上送到安全态势感知平台进行威胁分析。

5.6.4 设备安全

网络设备的安全可信是指网络设备在保障安全性（机密性、完整性和可用性）的同时，具备让用户信任其隐私保护、可靠性和稳定性的能力。网络设备的安全可信对于个人隐私、企业运营、国家安全、数字经济发展以及全球网络空间治理都具有极其重要的意义。因此，我们必须高度重视网络设备的安全可信问题，采取有效措施加强网络设备的安全管理。

从园区网络威胁看安全要求，需重点保护终端和服务器上软件、数据、硬件等关键对象，设备安全覆盖管控平台软件、路由器、防火墙、交换机和 WLAN 等产品。

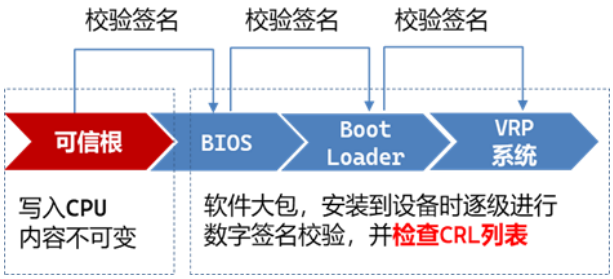
图5-17 园区网络威胁示意图

从网络设备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

安全启动：设备以硬件可信根为信任起点，前一个部件逐级验证下一级要加载的软件的签名，保证启动过程加载的软件没有遭到黑客或者恶意软件篡改。

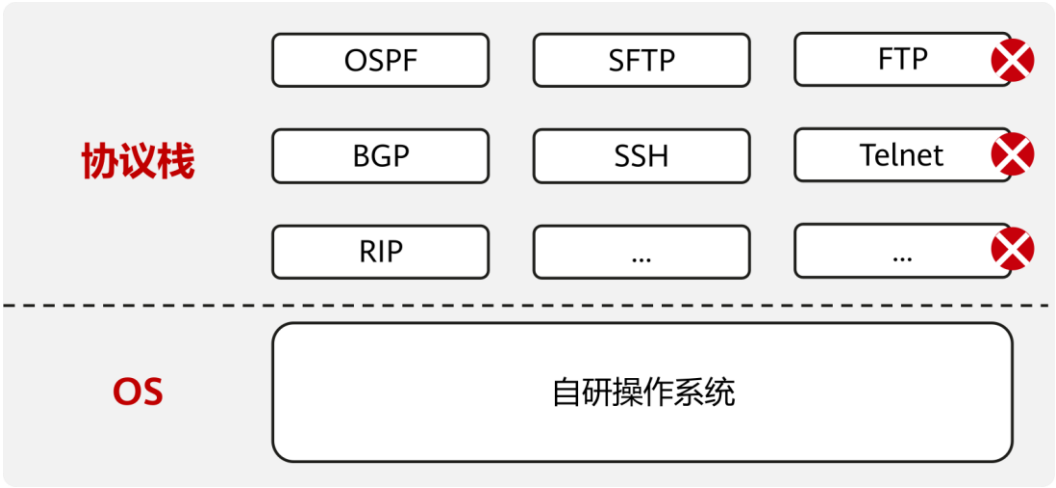
图5-18 签名校验过程



协议安全

默认出厂版本只支持安全协议和算法（协议标准不支持安全算法除外），最大程度的保证默认状态安全，支持更安全标准的 SZTP，实现设备零配置安全入网。

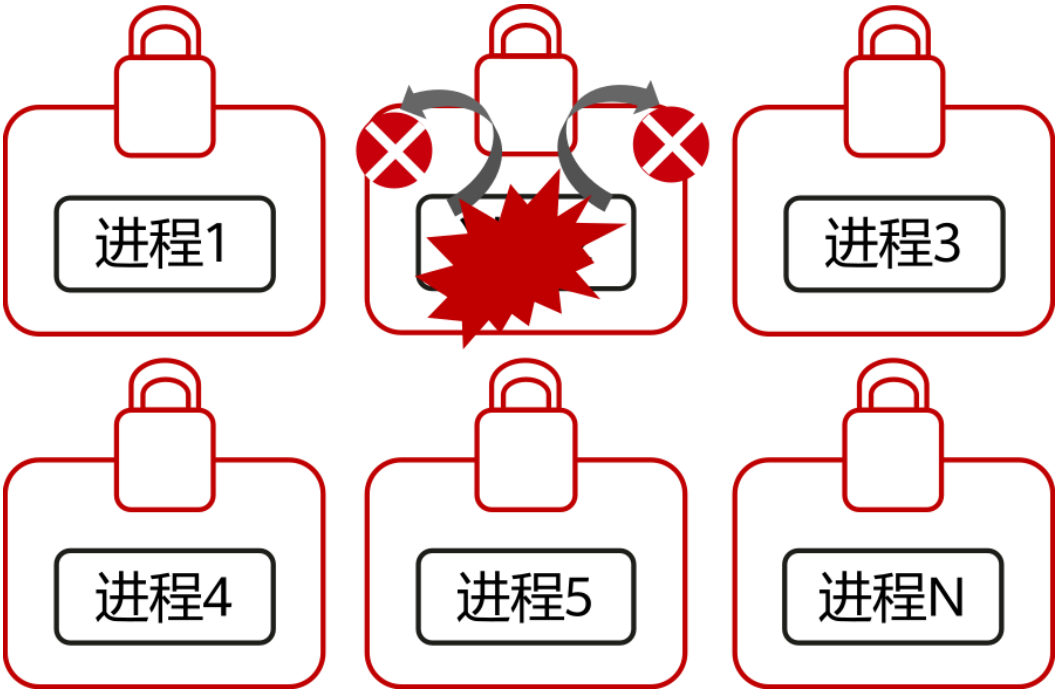
图5-19 不安全协议



威胁防扩散

进程根据业务需要使用最小的权限，严格控制 ROOT 权限使用，对于需要特权的业务进程通过白名单等技术手段实现权限限制。避免被攻破后横向影响其他进程或设备。

图5-20 进程权限控制



5.6.5 关键指标

园区网络部署上述的终端、设备、链路、设备安全功能后，建议网络达成如表 5-5 所示安全能力。

表5-5 零信任关键指标

分类	指标项	推荐值	基础达标值
终端安全	AP 和交换机支持内置终端识别能力，针对国内市场占有率 TOP5 的办公哑终端、摄像头、打印机、IP 话机进行精准识别	设备内置终端识别能力	非设备内置终端识别能力
	终端异常检测，支持仿冒终端识别、告警、自动阻断	设备内置终端异常检测能力	非设备内置终端异常检测能力
	网络设备内置终端防私接，识别 HUB、路由器、Wi-Fi 热点共享私接	设备内置防私接能力	非设备内置防私接能力
	业务策略与 IP 解耦，位置变化无需重新部署安全策略	支持	支持
链路安全	无线 AP 空口报文加扰防窃听	支持	不支持
	园区有线 AP-接入-汇聚-核心端到端 MACsec 加密	全支持	部分支持
设备安全	开局安全：支持 SZTP	全部支持	不支持
	协议安全：BGP、OSPF、ISIS 支持国密算法和 HMAC 认证，BGP 支持 TLS 认证，MD5 认证不安全风险提示	全部支持	支持国密算法，默认安全
	安全配置核查：支持不安全的协议和算法、异常端口开启、账号口令策略、全零监听等配置核查，提示风险和修复方案	全部支持	不支持
	态势感知：主机入侵检测 HIPS：识别异常网络设备登录如暴力破解、非授权账号登录、非常见路径登录、登录频率异常等，识别文件权限提升、关键文件篡改、shell 文件篡改等异常安全事件，形成安全日志、并进行威胁分析，生成威胁事件通告	全部支持	不支持

5.7 基于多级节能构建绿色网络

5.7.1 网络绿色低碳

园区网络节能需要从设备级、网络级以及系统级三个方面考虑，逐级构建绿色低碳的园区网络。

设备级节能

设备级节能是绿色低碳园区网络的基础。首先，选用低功耗、高性能的网络设备，如交换机、路由器、无线接入点等，降低设备在运行过程中的能源消耗。其次，采用先进的节能技术，通常包括风扇智能调

速、激光器自动关断（ALS，Automatic Laser Shutdown）、能效以太网（EEE，Energy Efficient Ethernet）、端口休眠、关闭冗余电源、智能休眠、动态功率管理等，使设备在空闲或低负载状态下自动降低功耗，从而提高设备利用率，减少能源浪费。设备级节能还包括对设备的运行状态和功耗进行实时监控，通过智能算法调整设备的工作状态，以匹配实际的业务需求，避免资源浪费。单设备至少具有如下节能模式：

- 基础休眠：针对有长时段容量轻载，用户不是常驻，并且接入随机特征的局部区域，设备支持进入基础休眠，设备此时能够提供基础的接入能力。
- 深度休眠：设备支持关闭绝大多数器件，仅消耗极小功耗，无接入能力。但是设备具备感知能力，在感知有终端/人员用网时，快速唤醒设备。

网络级节能

网络级节能是绿色低碳园区网络的关键。园区网络需实现整体优化，降低整体能耗。

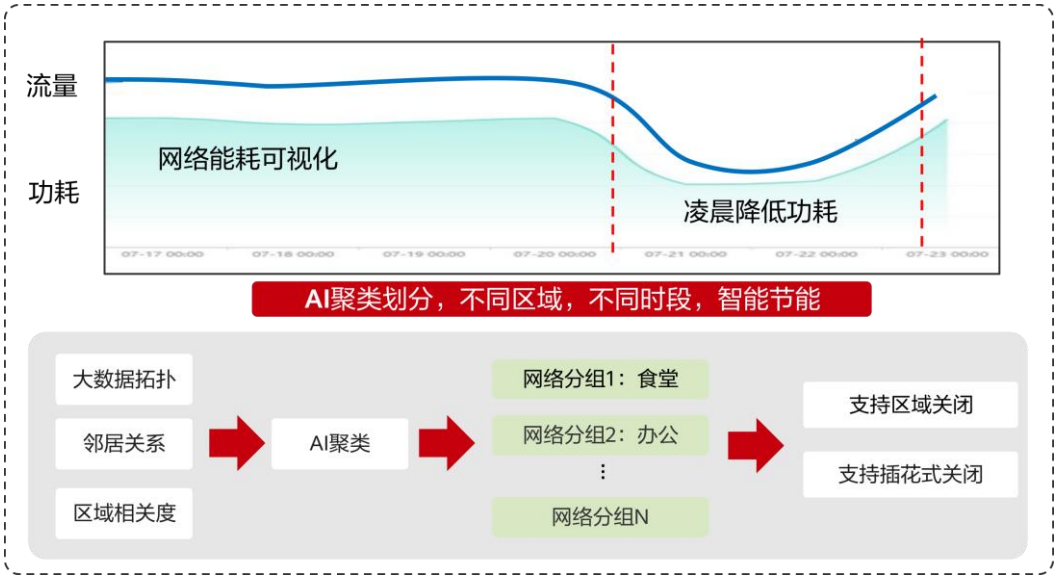
一方面，通过合理规划简化网络架构，如将三层架构变两层架构，采用 VXLAN 虚拟化、网络切片等技术，实现网络资源的按需分配，提高网络资源利用率。

另一方面，运用网络级节能策略，如负载均衡、流量调度等，降低网络设备的空载功耗，减少碳排放。通过网络协同联动机制，使得每台设备的节能状态不再独立；从全网角度来看，网络轻载时，大部分设备处于深度休眠，少部分设备处于基础休眠，使得网络兼具节能能力和基础可用性。

系统级节能

系统级节能是绿色低碳园区的最高目标，要求园区网络的各个方面，包括设备、网络和管理平台，都要协同工作，形成一个统一的节能系统。系统级节能需要建立一个全面的能源管理系统，通过集成的监控和分析工具，自动识别对不同场景选择合适的节能模式，如图 5-21 所示，实现对园区网络能源消耗的全局掌控。系统级识别不同区域、区域内局部的流量潮汐变化，智能选用节能模式：对于整片区域处于轻载状态时，以深度休眠为主；在整片区域内的局部轻载时，以基础休眠为主；如果整片区域的网络负载不断变化，需结合深度和基础休眠，合理调配。同时，节能策略推荐时自动划分小区选取监视 AP 保障基础覆盖，自动识别网络容量增长趋势唤醒节能 AP。

图5-21 系统级节能



这个系统能够跨设备和网络收集数据，评估节能措施的效果，并提供决策支持，帮助园区管理者制定更加有效的节能策略。

5.7.2 网络能耗可视化

整体园区网络的能耗可视是节能的基础功能，可对园区网络交换机，WLAN AP，WLAN AC 等设备的能耗进行可视化呈现。园区分析器需提供丰富的能耗可视，包括指定区域的**能耗趋势、能耗分布**（如图 5-22），指定时间段的节能前后**能耗对比**（如图 5-23）等。园区设备的能耗数据通过 Telemetry 上报到分析器，分析器依据能耗数据计算出能效比（GB/KWH），并可多粒度的在数字地图上呈现能耗数据，包括整网级、站点级、设备级、单板级和端口级，还可以依据历史数据可呈现能耗趋势，能耗对比数据。

图5-22 能耗趋势和能耗分布图

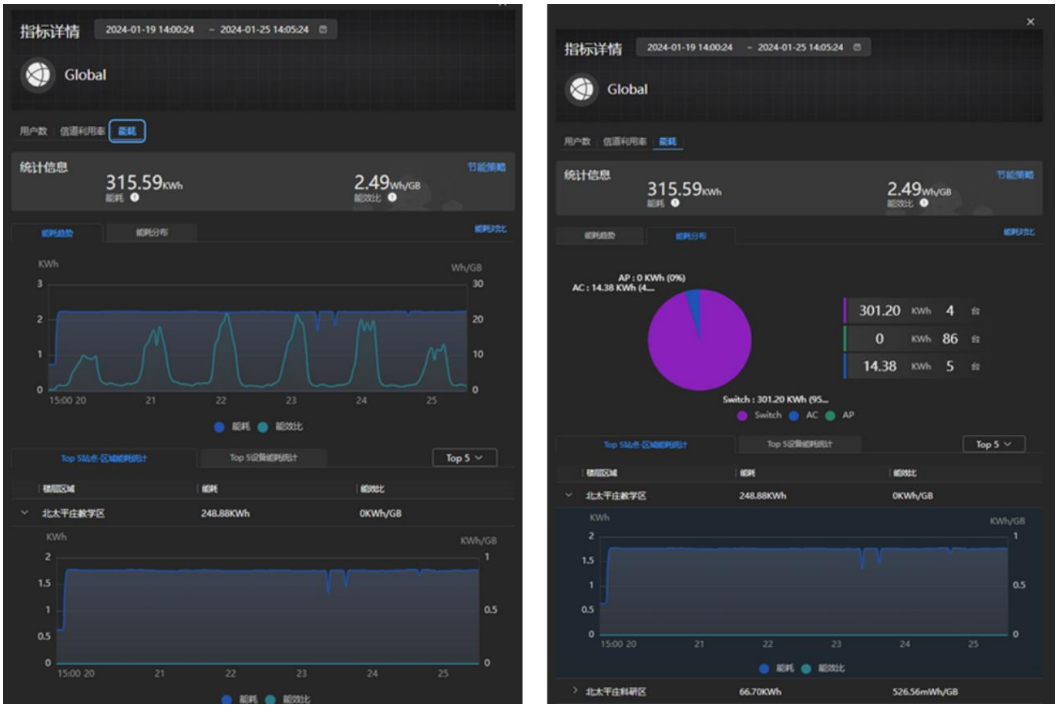


图5-23 能耗对比图

5.7.3 关键指标

绿色低碳园区网络建议指标如表 5-6 所示。

表5-6 绿色低碳关键指标

分类	指标项	推荐值	基础达标值
网络节能	免人工规划，自动感知网络潮汐特征，推荐保障 AP、节能 AP 和节能时段；节能时段内基础覆盖和物联业务不中断	支持免人工规划，自动推荐节能策； 节能不影响物联业务；单台 AP 节能态对比待机状态，能耗降低 70%以上	支持周期性 PoE 关断 AP 节能
系统节能	无需 Wi-Fi 接入，利用 AP CSI 感知空间人员有无，对电灯和空调的关断	支持	不支持

6 总结

本文从企业园区业务发展趋势出发，总结出未来园区网络万兆超宽、确定可靠、体验保障、智能运维、安全防护及绿色低碳六大需求。根据未来园区网络需求，再进一步总结出实现需求的关键技术，并提出高品质万兆园区的概念、建网方案、建网标准及分级指标建议。

高品质万兆园区网络是具备万兆超宽、确定可靠、体验保障、智能运维、安全防护、绿色低碳能力的下一代园区网络，Wi-Fi 7 和万兆接入技术是其显著特征，同时还需要实现以体验为中心的建网架构，以满足应用体验的提升、用户体验的提升以及运维体验的提升。园区的安全防护能力和绿色低碳能力，也是高品质万兆园区所必须具备的能力。

本文对园区的普适性场景做了分析与总结。但各个区域、各个行业还有其特点，对园区网络有特定的网络质量要求，或特定的网络安全防护要求等。同时各个区域的能源现状不同，用电费率不同，绿色低碳能力对其园区网络的重要性和紧迫性也不同。本文无法面面俱到的完成所有分析，后续还需要分区域、分行业进行进一步研究和分析。

A 缩略语

表A-1 缩略语

缩略语	英文全称	中文全称
AI	Artificial Intelligence	人工智能
XR	Extended reality	扩展现实
PC	Personal Computer	个人电脑
VR	Virtual Reality	虚拟现实
AR	Augmented Reality	增强现实
VPN	Virtual Private Network	虚拟专用网
AP	Access Point	接入点
CT	Cycle Time	周转时间
VIP	Very Important Person	重要用户
DSCP	Differentiated Services Code Point	区分服务编码点
AGV	Automated Guided Vehicle	自动引导运输车
LAN	Local Area Network	局域网
WAN	Wide Area Network	广域网
OPEX	Operating Expense	运营支出
SDN	Software defined Networking	软件定义网络
QAM	Quadrature Amplitude Modulation	正交幅度调制
RU	Resource Unit	资源单元
WLAN	Wireless Local Area Network	无线局域网
TCO	Total Cost of Operations	总成本
PHY	Port Physical Layer	端口物理层
WDM	Wavelength Division Multiplexing	波分复用
PON	Passive Optical Network	无源光网络
PoE	Power over Ethernet	以太网供电
VXLAN	Virtual Extensible Local Area Network	虚拟扩展局域网

缩略语	英文全称	中文全称
VN	Virtual Network	虚拟网络
BGP	Border Gateway Protocol	边界网关协议
EVPN	Ethernet VPN	以太网虚拟私有网络
SRv6	Segment Routing over IPv6	基于 IPv6 的段路由
SLA	Service Level Agreement	服务水平承诺
TSN	Time Sensitive Networking	时间敏感网络
OT	Operation Technology	操作技术
PLC	Programmable Logic Controller	可编程逻辑控制器
I/O	Input/Output	输入/输出
IT	Information Technology	信息技术
FlexE	Flexible Ethernet	灵活以太
HQoS	Hierarchical Quality of Service	分层服务质量
M-LAG	Multichassis Link Aggregation Group	跨设备链路聚合组
MSTP	Multiple Spanning Tree Protocol	多生成树协议
HSR	High-availability Seamless Redundancy	高可靠性无缝冗余
ERPS	Ethernet Ring Protection Switching	以太网环保护
RPL	Ring Protection Link	环路保护链路
HTTP	Hypertext Transfer Protocol	超文本传输协议
FTP	File Transfer Protocol	文件传输协议
QoS	Quality of Service	服务质量
EDCA	Enhanced Distributed Channel Access	增强型分布式信道访问
FEC	Forward Error Correction	前向纠错
ZTP	Zero Touch Provisioning	零配置部署
SD-WAN	Software-defined Wide Area Network	软件定义广域网
ARP	Address Resolution Protocol	地址解析协议
OSPF	Open Shortest Path First	开放式最短路径优先
MIMO	Multiple-input Multiple-output	多输入多输出

缩略语	英文全称	中文全称
IETF	Internet Engineering Task Force	互联网工程任务组
AH	Authentication Header	认证头
ESP	Encapsulating Security Payload	封装安全载荷协议
IPS	Intrusion Prevention System	入侵防御系统
AV	Antivirus	防病毒
NAT	Network Address Translation	网络地址转换
CSI	Channel State Information	信道状态信息
ALS	Automatic Laser Shutdown	激光器自动关断
EEE	Energy Efficient Ethernet	能效以太网