



迈向智能世界白皮书

数据通信

联接无处不在的
算力和智慧生活



构建万物互联的智能世界

序言

人类社会正处在迈向智能世界的关键历史节点。智能世界需要通过数字化和智能化构建。

数字化和智能化浪潮也正在给全球企业掀起新一轮的变革。面对日益复杂的内外部环境、不断多样化的客户需求和业务场景，企业 IT 迫切需要以低成本、高敏捷、灵活弹性和支撑业务及技术创新为目标进行数字化选型。从全球看，企业 IT 正在发生如下变化：

1. 多云化成为企业共识：多云架构集成了私有云和多个公有云。多云使得企业可以根据不同时空的业务和安全需求灵活分配托管策略，从而充分利用多云的规模经济、灵活性、可扩展性等特点，实现降本增效；
2. 物联网走向规模部署：无论是高效便捷的办公环境，高效安全的工业生产、紧张繁忙的公共交通，还是天空、地面的物流系统和千行百业的楼宇等等，物联网技术都扮演愈发重要的战略作用。作为通信和互联网的延伸，物联网利用感知与智能技术，使得企业和个人以数字化手段对物理世界实时控制、精确管理和科学决策；
3. 混合办公成为新常态：虽然大部分国家已进入疫情恢复状态，但远程办公已成为常态化，目前有超过 80% 的员工希望他们的雇主继续支持远程工作。但远程办公带来数据安全风险，钓鱼攻击、勒索病毒导致的数据泄露成为当前企业最大的安全隐患，企业越来越希望将安全产品整合到多功能解决方案中，以应对一系列广泛的相关挑战；

4. IT 运维难度日趋增加：在移动化、大数据、云计算、人工智能等新技术的推动下，企业的 IT 基础架构所涉及的网元数、技术栈、服务数等元素成倍剧增。而当前企业 IT 系统缺乏数字化技术，运维人力能力不足、网络缺乏可视化手段、海量无效告警等都导致业务故障定位效率低下，严重影响业务体验。

这些变化促使企业数据通信网络架构的变革。回顾过去，数据通信网络的发展经历了学术研究、万维网应用、社交媒体与多业务承载、短视频与移动互联以及云时代与行业数字化五个阶段，未来的世界是万物互联、万物智联和万智互联的智能世界，数据通信网络支撑的应用场景持续丰富，我们认为网络将进入一个 5.5G 时代，聚焦多云协同、泛在物联、超自动化、确定性体验、网络安全服务化、超融合数据中心这几个关键趋势持续演进。本文结合业务变化对网络带来的挑战，以及网络技术代际演进，对于构筑面向数字化、智能化时代的网络给出行动建议。同时对数据通信网络的未来发展进行了展望，即全面迈向 Net5.5G 时代，助力企业快速抓住行业趋势和变化，通过数字化手段打通内外数据通道，实现数据共享与数据整合，完成高效数据价值挖掘，在瞬息万变的市场上取得先机。

胡克文
华为数据通信产品线总裁



目录

CONTENTS

趋势一01

云原生的多云弹性
网络成为企业 IT 云化是否
成功的核心

趋势二08

物联网从面向轻量
数据采集的简单业务
走向高密采集 + 控制协同的
复杂业务

趋势三15

基于云的网络安全服务
方案日趋成熟

趋势四21

数据中心网络正在向
全以太网化演进

趋势五27

基于人工智能的
超自动化正在改变
网络管理方式

趋势六34

工业网络走向 IT/OT 融合
使能工业智能化升级

展望38

联接无处不在
的算力和智慧生活

01

云原生的
多云弹性网络成为
企业 IT 云化
是否成功的核心



 趋势

随着企业应对日益复杂的内外部环境变化、客户需求及新的业务场景不断增长，多样化、个性化和高效化驱动企业以低成本、高敏捷、灵活弹性、支撑业务及技术创新为目标进行数字化选型。随着云计算产业不断成熟，大多数企业选择将多云战略纳入其长期规划，IT部门对公有云及本地私有云的部署都在不断增长。根据Flexera的“2021 云状态报告”

显示，全球已有92%的受访企业采用了多云战略，平均用云数达5.3个，其中使用混合云部署模式的用户比例高达82%。但大规模的企业应用向多云转型并不像想象中的那么简单。多云应用的关键能力是异构多云管理，而多云间的网络互通管理是最大的挑战，面向多云原生的网络架构应解决易用性、可靠性以及安全性等问题和需求。

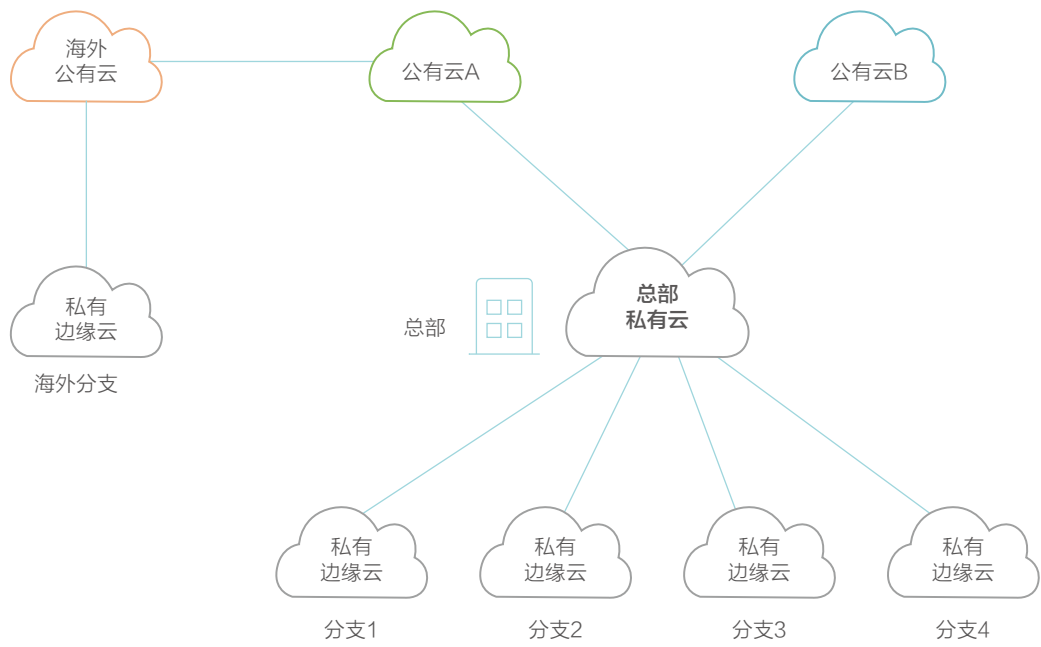


图1 典型企业多云组网



挑战

多云带来如下网络问题：

- 1. 网络的碎片化难以保障业务体验：**多云架构打破了经典的LAN/DCN/WAN的架构和对应的知识和经验，引入了不同云服务商的多个云上虚拟网络，而不同云商提供的云上虚拟网络技术栈不统一，例如VXLAN、GRE、L2TP等，跨云网络管理需要使用不同工具和协议，现有IT系统难以统一拉通各个网络的管理、配置、监控和运维，面临业务体验的投诉时需要在多段网络孤岛寻找问题所在，疲于奔命；
- 2. 网络的运营效率受到挑战：**实现云间互通当前普遍通过云上的API互联，不同云上API、参数等差异较大，企业需要通过统一接口对接，实现复杂。这给企业IT团队带来如下挑战：理解多云网络的各自特点来决策自身方案带来的过高学习成本；频繁按照云商的技术变化带来的IT系统的整改升级。这些挑战



推动了IT运营成本的升高；

- 3. 网络安全与合规更加复杂：**多云的应用导致暴露面增多从而导致攻击面增多；导致失去集中的访问控制和权限管理；导致更加繁重的数据治理任务来防止数据泄露和滥用；企业需要保证私有云上的传统安全策略和企业定制化的安全架构在私有云上得到统一的继承和实现。
- 4. 网络的连接成本持续攀升：**数据流从本地私有IT扩展到多云需要远距离高带宽的网络连接。如果仅依赖运营商专线则面临持续攀升的数据传输成本。如何利用好带宽更大且成本更低的互联网资源成为迫切需求；



建议

层次化架构，屏蔽多云异构网络差异，实现多云网络统一运营

- 1. 网络连接的层次化拉通：**网络层次化将网络分为异构基础网络层、多云虚拟网络层和租户视角的业务连接层。层次化架构的好处在于：向下提供对物理网络连接的管理和运维；向上屏蔽异构网络的差异，以业务视角按需提供云下到云上、多云之间的无缝网络连接和业务保障；
- 2. 网络运营的统一化：**屏蔽多云的网络运营差异，全生命周期提供全局集中式的多云、多站点的统一网络编排和策略管理、故障恢复和高可用性，以及配置和运行状况可视化监控，实现云间联接、带宽和应

用基于业务意图的按需自动发放；

时实现最优资源利用效率、成本可视化；

3. 安全随行：提供云原生的SD-WAN/SASE能力，统一身份、分析、策略等，安全内置到网络架构，实现云网端一体的E2E数据流行为安全管控；

4. 网络资源的高效利用：精细化服务质量感知、全维度细粒度遥测，基于实时感知配合控制器实现云间的资源调优，保证业务体验的同
5. 业务应用的质量保障：具备应用识别、数据流识别，基于不同应用，提供差异化的网络服务，例如数据加速，确定性无损体验保证，资源极速调用、应用流量治理、网络/应用/数据高可靠；

6. 开放易运营：多租户服务、应用级单流运营、开放的层次化网络服务、智能推荐；

解决方案

华为 iMaster NCE-Fabric 混合云解决方案

针对多云之间的灵活网络编排与安全合规痛点，华为推出了 iMaster NCE-Fabric 解决方案。其总体逻辑架构可分为业务编排层、控制层、基础设施层。

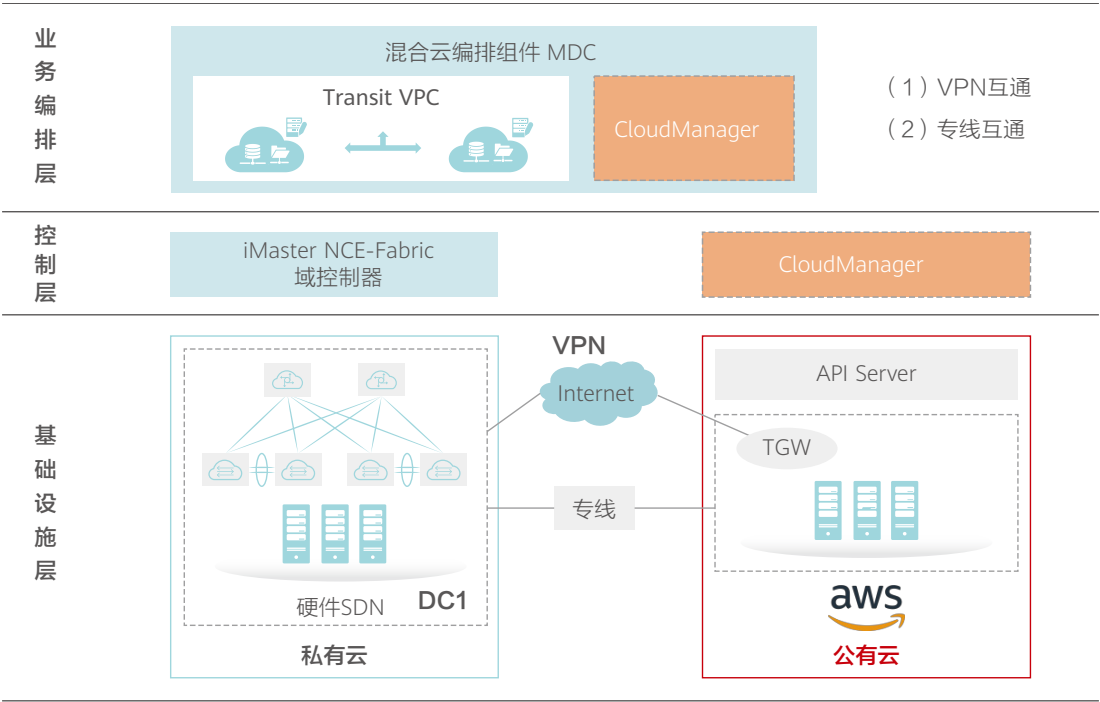


图2 华为iMaster NCE-Fabric混合云解决方案全景图

1. 业务编排层：混合云编排组件Multi-Datacenter Controller(MDC)，用于屏蔽异构的多云之间的差异性和复杂性，使得业务部门聚焦业务系统的连通性，对公有云、私有云的业务互通网络编排和安全隔离以及合规要求；
 - MDC：Multi-Datacenter-Controller，多数据中心控制器。支持私有云跨Fabric业务互通编排、私有云与公有云之间的业务互通编排以及灵活的安全策略控制；
2. 控制层：对公有云、私有云的域内网络编排，配置自动化下发，以及统一运维，其中iMaster NCE-Fabric和CloudManager分别负责私有云和公有云的网络编排；
 - iMaster NCE-Fabric：私有云域控制器，南向负责管理私有云内单个或多个Fabric内物理设备，编排并下发Fabric内的逻辑网络；
 - CloudManager：公有云网络编排，南向远程调用公有云开放API，完成对公有云网络的配置下发；
3. 基础设施层：包含一个或多个云内网络，提供异构云互通Overlay网关，通过专线或VPN，与公有云连接。



客户价值

iMaster NCE-Fabric 混合云解决方案的价值：

1. **部署简单**：不需要在公有云内部署云化控制器和虚拟化网元设备，也不需要额外创建公有云管理账户，私有云内通过远程调用公有云API的方式完成对公有云的配置发放和状态监控，组网架构上多云解耦，同时也减少公有云使用成本。

2. **灵活编排**：统一的公有云、私有云互通网络编排界面，支持使用图形拖拽方式编排逻辑网络，逻辑拓扑可视，减少在不同菜单编排页面间反复切换，提升编排效率；
3. **网络可视**：支持公有云网络拓扑可视，对已经下发的公有云网络配置进行配置上收并将配置还原为逻辑拓扑展示，在网络资源对象众多时，为管理员提供了一种方便快捷的查看网络资源对象之间的关联关系的视图。



解决方案

华为多云增强的 SD-WAN 解决方案

针对企业提供分支与分支、分支与数据中心、分支与云之间提供全场景按需互联的需求，华为推出全新升级的增强 SD-WAN 解决方案，实现应用级智能选路与智能加速、智能运维，构建更好的业务体验，重塑企业 WAN 互联全流程的业务体验。华为多云增强的 SD-WAN 解决方案由网络层和管理层组成：（图 3 华为 SD-WAN 解决方案全景图）

1. 网络层：
 - 提供多种有线和无线接口，支持丰富的组网模型；
 - 支持多租户，管理和数据全隔离；
 - 提供云原生的SASE安全服务能力，支持多云的虚拟化网关部署；
 - 支持物理CPE & vCPE两种方式；
2. 管理层：
 - iMaster NCE 控制器：对网络设备进行集



图3 华为SD-WAN解决方案全景图



客户价值

华为多云增强的 SD-WAN 解决方案的价值：

1. **一网多云：**支持多种组网模型，满足不同分支网络需求，支持华为云、阿里云、腾讯云、AWS、天翼云、微软云等主流公有云部署，实现本地、公有云互连，统一纳管，策略统一编排；

2. **智能选路：**基于应用SLA、应用优先级、带宽利用率等多维度综合路径选优，保证关键应用在最优链路上；内置首创A-FEC质量感知，确保30%丢包率下的音视频应用无损体验；

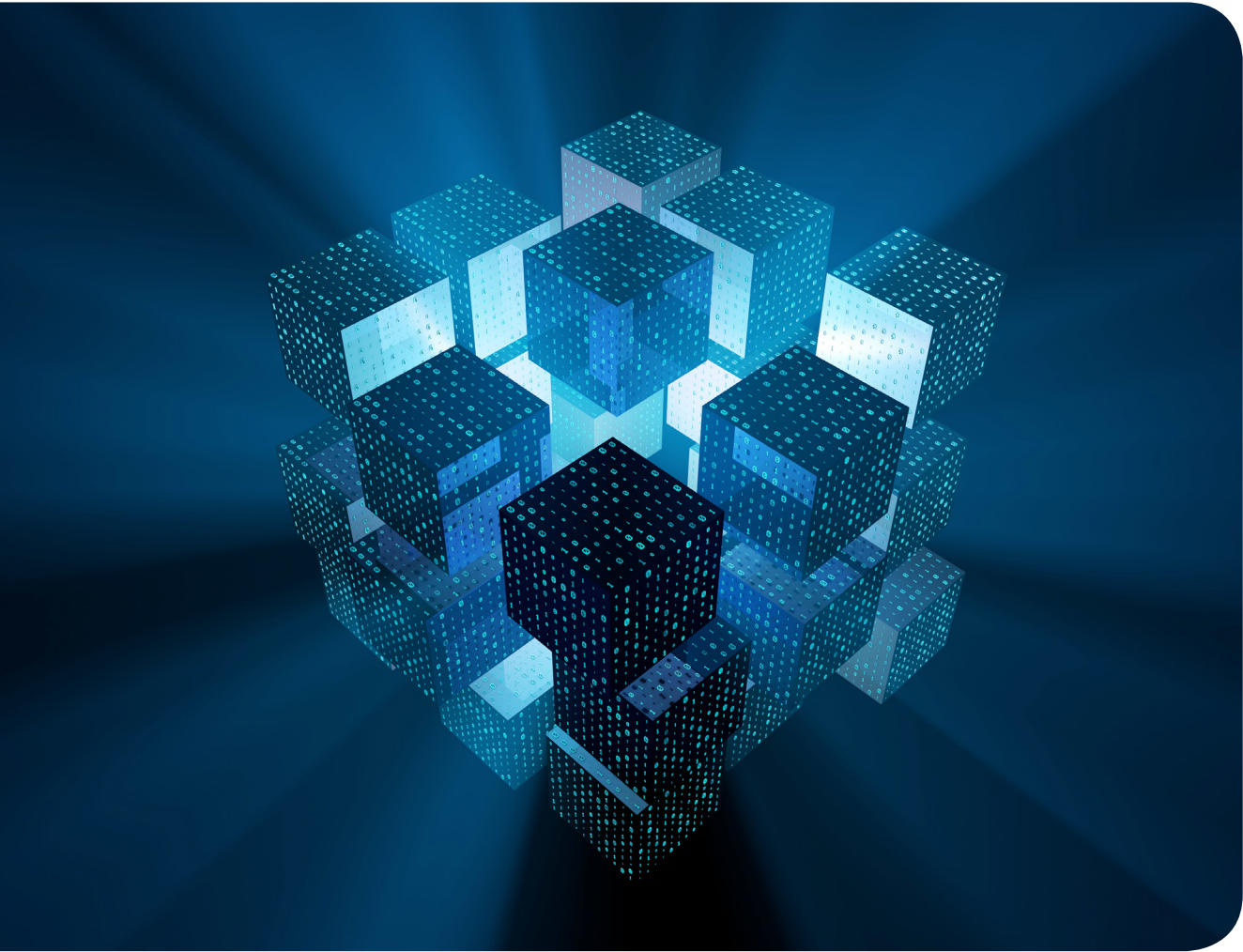
3. **品质卓越：**最高支持10Gbps SD-WAN性能，满足高性能HUB、IWG部署诉求，支持5G移动网络上行，支持逐包/逐流负载分担，提升网络可靠性；

4. **安全扩展：**内置7层应用识别控制、Firewall、

IPS、URL过滤、Anti-Virus等特性，无需额外设备，统一企业上云安全策略，支持高级安全功能，例如威胁感知、恶意文件识别、异常攻击防护等；

5. 智能运维：基于智能和大数据分析技术，通过Telemetry 技术实时采集网络数据，利用大数据分析、机器学习算法学习网络行为并识别故障模式。主动发现85%的网络问题，提供智能的根因分析，打造卓越的网络服务保障体验。

华为 SD-WAN 解决方案提供强大组网、优质体验和简易运维的能力，满足小型、中型、大型甚至超大型企业和运营商、服务提供商的多云互联需求，NetEngine AR 及 SD-WAN 服务全球 50000+ 客户，解决方案荣获 2021 年 Gartner 客户之选。华为 SD-WAN 解决方案为企业提供优质的上云体验，同时提高了企业分支网络的可靠性、灵活性和运维效率，确保分支网络永久在线，保证业务的连续和稳定。



02

物联网从面向轻量
数据采集的简单业务
走向高密采集 + 控制协同
的复杂业务





趋势

在当前数字化建设过程中，企业往往面临缺乏基于实体的真实数据，存在数字触点不够、无法支撑在数字空间构建与实体精准映射的数字孪生系统等问题。物联网是任何实体设备数字化、智能化的基础。根据GSMA预测，到2025年，全球物联网总连接数规模将达到246亿，年复合增长率将高达13%，产业物联网设备联网数将在2024年超过消费物联网设备数。企业借助物联网可以获得更多数据来提高生产效率。随着5G、Wi-Fi 6E技术以及生态的不断成熟，物联网正从面向轻量数据采集的简单业务，走向高密采集+控制协同的复杂业务。不仅需要满足零售、教育等场景下普通的物联网场景需求，而且已经开始逐步渗入到智能制造、电力控制、港口等生产环节，对物联网的连接提出更高要求：

1. 工业4.0越来越依赖物联网：如果没有物联网，提高工业能力所需的大规模数据收集和监控将是不可能的。头部汽车工厂在大量使用机器人和AGV的同时，通过大数据平台连接了2万+各类摄像头、仪表、传感器，实时监控和分析生产过程。为满足生产过程高度智能、柔性化和透明，生产要素之间需实时同步与交互，连接需要达到

99.999%的可靠性和毫秒级时延，同时工厂复杂环境下，对于终端抗干扰的定位技术也提出了更高的要求；

2. 医疗物联网（IoMT）持续发展：医疗物联网通过患者和医务人员、医疗机构、医疗设备之间的连接和互动，实现患者与设备数据标准化采集与分析、医疗废弃物跟踪、高价值资产盘点、患者手环检测、输液检测、医疗耗材跟踪、轮椅类器械定位等。头部医院已经实现400多种、15万余台低功耗医疗设备联网，支持轨迹与状态信息实时展示，大幅提升医护效率；

3. 智慧城市大规模建设：城市物联是智慧城市的基础，结合人工智能技术，提升城市管理水平。通常而言，城市物联网的规模可达到上百万，以上海市物联网中心一期为例，接入7区近百类、510万个设施，日产生数据超过3400万条，未来将增加到千万感知终端。对于智慧城市的复杂环境，尤其是水库、气象、电力等场景，无电无网下的低功耗数据回传成为刚需；



企业部署物联网面临如下挑战：

- 1. **终端联网率低：**联接是实现行业数字化的第一步，当前存量老旧设备多，尤其是生产制造领域，设备联网率仅为20%，越到末端联网率越低，数字化水平不高直接导致数据采集难、成本高、效率低；
- 2. **数据互通难：**传统的物联网系统独立建网，不同的物联终端厂商不一，通信接口、通信协议差异很大，子系统大多采用非IP布线方式，需要通过协议转换才能进行数据交互。IT网络和OT网络割裂，导致系统之间数据不通，无法有效配合实现联动。需要打破物联网的信息孤岛，实现物联终端之间的语义互通，数据共享，互相联动，发挥数据价值；
- 3. **部署调试复杂：**不同的场景下对传感器的感知技术、环境适应性和通信技术要求不同。大部分物联终端组网后，还需要和IT网络互通，将数据传输给大数据平台进行统一处理。在部分场景下部署物联终端需要挖沟开槽，安装工期长，部署调试复杂，施工要求多，成本巨大；
- 4. **网络运维困难：**物联网具有终端数量多，线路复杂，覆盖范围广，点位分散等特点，而且大量传感器为哑终端，一旦出现故障，面临排查工作量大，效率低，故障恢复时间长等问题。需要实现在超大规模组网下的智能化高效运维、优化连接体验；

- 5. **安全可靠：**物联终端分布广，尤其是哑终端几乎没有安全防御能力，使得物联网容易成为网络安全入侵和安全攻击的对象。随着物联网规模的而不断扩大，对设备准入和物联终端冒仿的安全行为识别诉求越来越高。



提供更简单的组网和互通、更安全的接入和管控以及更智能的边缘计算能力，实现数字信息的泛在互联，高效通信

- 1. **统一简化接入技术：**通过技术改造，实现各类不同的连接方式统一，打破现有多种系统独立组网，相互孤立的现状，避免各种私有协议在网络中的规模使用，导致网络过渡复杂。
 - **有线接入统一到以太，降低布线成本。**
物联网市场存在各种线缆类型，如RS232、RS485、RJ45、USB、CAN等，建议将不同的接口类型统一到以太网技术，提升运维效率。以太网网络可以同时支持P2P，P2MP等多种连接方式，并且提供10Mbps/100Mbps/1Gbps多种速率的大带宽传输，还可通过双绞线向终端供电，从而降低线缆的部署成本与布线复杂度；
 - **无线接入以Wi-Fi为中心，融合多种技术协同。**随着 Wi-Fi 6 无线技术的成熟和普及，其技术有以下优势：对于改造/扩容布线困难场景，能够实现单终端Mbps

级以上大带宽接入（如视频），在新建网络场景中，对于有弹性扩容诉求的设备部署，采用无线方式更易扩容，可满足物联网终端设备可移动的场景需求，比如会议室办公终端，送餐或安保等机器人等；

- **物联网协议统一到IP，实现统一互通。**以IP化的物理连接方式进行部署，比如 Wi-Fi 等技术，可以简化网络部署，实现物联网设备即插即用，为物联网协议的统一提供通信基础，实现物联网数据互联互通，对于不支持IP的终端，可以使用SDK的形式，在终端操作系统中集成轻量化IP协议栈解决，实现“方言”到“普通话”的升级。IPv6技术让海量连接也能够有充足的地址，是实现IP一网到底的基础。

2. 部署智能边缘网关：物联网会产生海量数据，而这些数据需要进行处理和分析才可以进一步使用。通过边缘计算网关，能够将计算服务移到更接近最终用户或数据源的地方。边缘网关是部署在网络边缘侧的网关，通过网络联接、协议转换等功能联接物理和数字世界。通过边缘计算网关，可以就近在数据获取侧进行数据的初加工，进行清洗，转换，压缩，提取关键值等操作。边缘网关通过扩展远程终端单元（RTU）或可编程逻辑控制（PLC），架起边缘和云之前的桥梁。

- **本地处理：**物联网需要拥有更接近物理设备或数据源实际位置的计算能力。为了能够快速对物联网传感器和设备生成的数据进行分析，从而加速响应或解决问题，需要在边缘进行分析，而不是将数据传回中央站点再进行分析；

- **开放容器：**边缘网关提供标准化开放API对接企业物联平台，实现物联应用的实时开通部署，基于开放容器平台，可加载各行各业APP，使能终端联动。

3. 采用集中化管控平台：部署物联网后，网络运行状态只在网络管理平台等专用工具上可见，决策层无法直观了解整体运行情况，影响扩容决策及对重大事项支撑。因此，有必要打通回传网络和物联网之间的管理通道，采用集中化统一管理平台，支持数据标准化、连接管理、集中运维，北向提供接口，通过IOC平台直观呈现出回传网和物联网运行状态，包括带宽利用率、终端数量、在线状态等。集中化统一管理平台包括网络管理平台组件、物联管理平台组件；

- **网络管理：**支持网络业务管理、网络安全管理、用户准入管理、网络监控、网络质量分析、网络应用分析、告警和报表等功能，提供大数据分析的能力，同时提供开放的标准接口、支持与 IOC 对接；
- **物联管理：**支持对终端类型、运行协议、ID、MAC 地址进行登记管理，同时对物联终端送上来的数据进行处理、存储、格式转换，并提供标准的接口给上层的 IOC 或者应用；

4. 利用人工智能提升安全：物联设备海量规模，完全依靠人力管理成本太大。当前物联系统可配置可操作性差，用户对终端安全意识不足。在海量接入、统一管控方面需要依靠人工智能、机器学习提升安全能力。

- **安全接入：**解决物联终端接入网络时仿冒或私接的问题，对于智能终端可以采

用内置安全SDK，采用二次认证方式安全接入，而对于无认证能力的哑终端，需要通过提取终端流量的特征信息，识别终端类型、厂家、SN等信息，只有符合业务类型的终端才放通网络权限，通过被动流量侦听智能识别未知资产和分类，系统可以自适应扫描识别具体资产，基于群体关系的无监督聚类算法，发现多种未知终端，对不同类别的未知类型终端进行归类，可以更加精准的进行安全接入管理；

- 安全管控：通过部署物联网防火墙、沙箱、探针等，实时分析整网的物联流量中的异常或畸形攻击报文、应用层恶意威胁流量，并上送安全态势感知系统，实现对整网的安全态势实时感知。引入无监督学习，分析流量智能识别异常行为，利用自学习的行为识别模型进行还原，发现仿冒/私接/被劫持终端，可以加速未知威胁诊断，主动阻断仿冒、被劫持、中毒终端。



解决方案

华为智简物联感知网解决方案：

智简物联感知网总体架构如图所示，由端、边、管、云四层组成：



图4 华为智简物联感知网解决方案全景图

1. 物联终端层：是物联感知网络的“末端传感”，联接着物理世界和数字世界，场景上主要分为两类。

- 室内为主的智慧园区物联感知类终端；
- 室外为主的智慧杆站物联感知类终端；

2. 边缘网关&感知接入层：物联感知网的“神经末梢”，决定整个解决方案易用性的关键。

- 向下联接着 OT 网络（支持 IOT 设备之间的操作指令通信的网络），可靠联接、业务本地存活；
- 向上联接着 CT 网络（支持 IT 应用数据通信网络），安全、可运维、可管理；

3. 回传网络层：是物联感知网络的“神经网络”，主要保障物联数据高效，可靠，安全的传输。

- 园区内网：采用VxLAN技术实现一网多业务承载，对不同的业务划分不同的虚拟子网保障业务隔离安全可靠；
- 广域回传网：可采用SD-WAN，优化投资性价比，实现对重要业务通过专网传输，对非重要业务可通过公网回传；
- 物联安全：部署安全防火墙实现对流量异常识别，畸形报文防护，对加密流量同样具备防护能力；

4. 云平台层：是物联感知网络的“神经中枢”，实现网络管理，安全管理，物联管理三大基本功能，既可以对网络设备进行管理，又可以对物联终端和业务的集中管

控平台，提供开放的标准接口，支持与IOC对接；

- 网络管理：主要包括智能运维、端网管理、网络管理等；
- 安全管理：主要包括HiSec安全态势管理、终端证书管理、统一登录等；
- 物联管理：IOT设备管理、IOT路由&规则引擎、物模型管理、插件管理



客户价值

华为智简物联感知网解决方案的价值：

1. 无感接入：通过IP化，能够实现 Wi-Fi 6无线接入和PLC-IoT接入，减少40%以上线缆的布置。采用无感接入技术手段进行自动引导，免去繁杂的现场配置，完成各类终端自动入网。做到物联终端设备一插入网，就可以进行业务通信。

2. 部署简单：华为Wi-Fi 6 AP提供物联插槽，可灵活扩展物联模块，方便快捷的实现蓝牙、RFID、ZigBee、UWB等物联网类协议功能扩展，广泛应用在企业资产管理、商超电子价签、城市智能环控、行业高精度定位等领域。多网合一部署、智能干扰避免等技术可以有效提升客户网络使用效率，TCO降低50%；

3. 一跳入云：通过边缘物联网关，将各种异构的物联协议进行标准化，将数据转换为云应用易懂的语言，使得物联终端接入边缘物联网关即可与云端应用实现直

接的数据互通，达到“一跳入云”的互通效果；

- 4. **一网可视：**通过标准接口对接，使能平台自动采集拓扑和状态数据，通过关联计算，生成回传网络和物联终端的拓扑及关联关系，使IOC具备全网联接及物联终端感知和呈现能力，包括全网拓扑、网络质量、终端状态、告警信息等；
- 5. **一体安全：**通过二次认证或者指纹识别解决物联终端设备防仿冒，保证物联终端的安全接入；网络设备能够识别并实现物联协议安全，并对数据采用加密传

输，避免物联数据流被窃取，篡改和重放攻击的问题，实现物联设备的安全通信；支持基于AI的整网安全态势感知与分析，实时阻断恶意流量，将有安全威胁的终端隔离下线，实现物联终端的安全管控。

华为的智简物联感知网，着眼于各个行业与用户业务紧密结合的物联网络，提供智慧化、便捷可靠的ICT解决方案，打造智慧、开放的网络和平台基座，为各个行业提供开放的生态环境，让各个行业的终端、业务系统和上层应用能够快速极简的方式部署到物联网络中。



03

基于云的
网络安全服务方案
日趋成熟





趋势

随着企业不断的数字化、云化，网络安全的重要性不言而喻，过去企业通常的做法是采用本地自行部署防火墙、IPS、沙箱、漏洞扫描、态势感知等多种安全产品实现网络防护，但是由于专业安全人员不足，很多企业并不能较好的应用这些安全产品从而达到良好的安全防护效果。部分安全产品上线后无人关注安全告警、缺乏及时调整安全防护策略，威胁数据库以及防护手段也不能持续升级，导致安全防护效果差强人意。而如今随着多云、物联、远程办公的盛行，网络安全的边界进一步扩大，勒索病毒盛行，且变得越来越有针对性，采用更加复杂的勒索策略，导致数据泄露等安全事故频发，传统的安全监控、检测和响应方法需要进行重大转变，以应对新技术和业务计划带来的风险。



挑战

企业传统网络安全部署中面临的挑战：

网络安全建设成本高：网络安全表面看起来是攻防之间的博弈关系，但实际是海量攻击手法

和海量防御手法之间较量，意味着企业或组织要想拥有较多的防御手法，就必须了解攻击的各个阶段，并根据各个攻击阶段评估下一阶段攻击手法，制定防御措施，因此通常为了达到防御效果，企业在网络安全上投入了巨大成本建立自己的网络安全体系，包括防火墙、入侵检测系统、防篡改系统、网络杀毒软件、网络行为管理系统等，但成本投入越大并不意味着网络越安全；

网络安全建设防御效果不佳：传统安全方案往往上报大量安全事件日志，有效和紧急的安全事件被淹没，安全产品各自为战，威胁分析片面，缺乏全局的统筹分析，难以达到威胁的准确识别和及时处置，而且网络安全防护的设备不能及时更新威胁库，服务能力和分析准确率受到影响，面对新的未知威胁，网络防御能力不佳；

网络安全工作需持续进行：从网络威胁生命周期角度来看，安全威胁事件的发生是没有时间规律的，具有明显的突发特征，即使部署了安全设备，在没有专业的安全管理流程和安全事件预警机制下，企业或组织的安全运维人员无法7*24小时监测企业或组织内部的网络安全状态，并及时响应；

安全人员能力不足：传统网络安全服务基本靠人支撑，属于重资产运营，对于网络安全维护人员的能力提出了很高的要求。在现实情况下，一个非以网络安全为主要产业的企业或组织难以培养网络安全领域的高阶人才。对于一

些中小企业或单位，专业安全人才的人力成本过高，这就造成了大部分中小企业或单位安全管理缺失、面对安全事件束手无策的局面；



企业通过本地安全能力与网络安全云服务结合，提升安全检测、分析、响应等能力，通过持续攻防对抗提升安全运营能力

随着企业对网络安全要求越来越高、可管理安全服务模式越来越成熟，解决方案从安全产品加本地驻场的运维模式走向基于云服务的模式，以云交付的形式提供网络安全防护能力势必成为网络安全投资的主流。云服务的日益普及使企业对采用云交付的安全解决方案更加开放。根据Gartner报告显示，到2024年，90%的托管安全提供商将放弃构建安全平台，转而采用SaaS模式的商用解决方案。

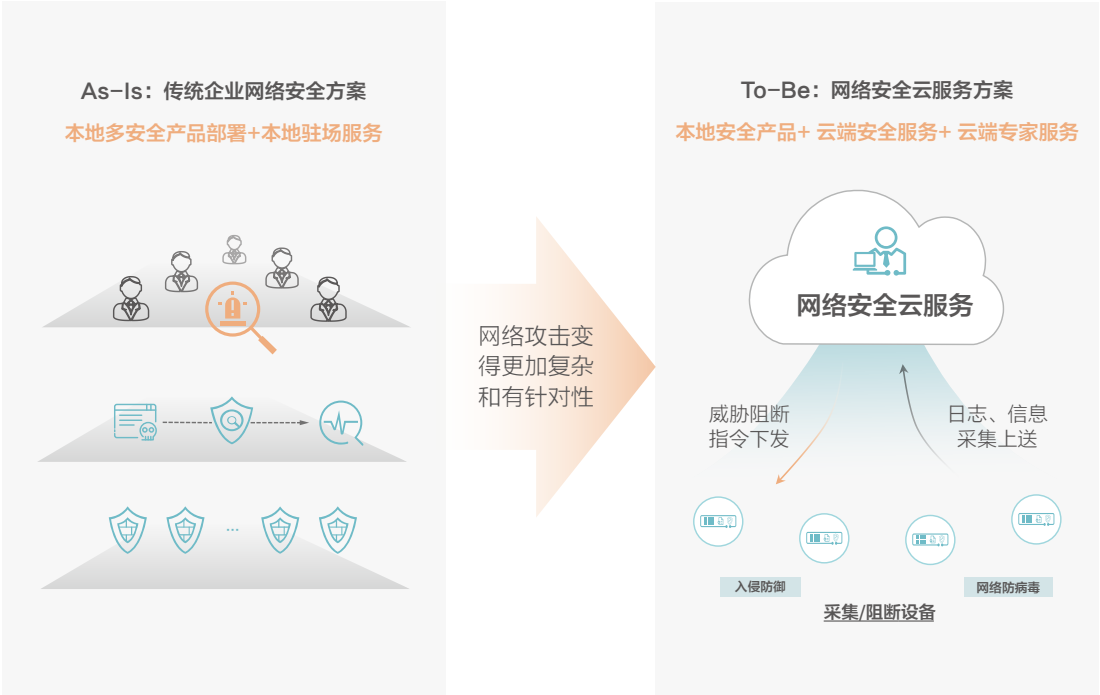


图5 网络安全服务演进

采用基于云的网络安全服务，企业只需要按需订阅，就可以获取实时、智能和精准的防护能力，加快网络安全部署时间，降低本地安全设备复杂度，同时也削减了大规模部署安全性相关的开销，包括运营成本以及相关IT资源，帮助企业解决日益复杂的威胁环境和缺乏熟练网络安全人员矛盾的问题。此外，企业现有的网络设备包括路由器、防火墙或 SD-WAN 可以连接到云交付的安全平台，在该平台上全局应用策略以确保一致的安全性和无缝的用户体验。

通过智能安全分析和自动处置算法提升安全分析人效，为客户提供高效、智能的安全代维服务，解决部分客户“不懂网络安全”的根本问题；通过广众的客户样本数据不断提升服务能力和分析准确率，降低安全设备整体的误报率，并通过云服务为有能力进行安全运维的客户提供安全咨询和安全工具服务，云端专家和自开发工具共享，提升用户体验，通过平台持续演进，达到安全能力平台化提供的目的，客户根据实际网络安全建设需要，按需订阅安全能力，满足多场景需求。



解决方案

华为乾坤安全云服务解决方案：

华为乾坤安全云服务解决方案由部署在华为公有云上的华为乾坤安全云服务平台和部署在客户本地网络的华为天关防护节点构成，实现云端服务+本地设备联动，构建简单、高效、易用的安全云服务方案。



图6 华为乾坤安全云服务解决方案全景

- **天关：**部署在客户本地的网络出口，可按需订购IPS、AV、URL和基于AI能力实现未知威胁安全防护能力，并同云服务平台联动，作为安全云服务的基础，其核心能力包括：

1. 具备全面的内容安全能力，如入侵防御、恶意文件检测等，为用户检测、阻断应用层攻击事件；
2. 配备华为安全人工智能AIE引擎，提供边缘侧的AI安全检测能力，能够检测传统基于特征签名无法完成的检测任务，例如：暴力破解、C&C、DGA、ECA等算法；
3. 实现与云服务平台的联动，上报安全事件相关的关键信息，并可以根据云服务平台的指令对安全事件进行闭环。

- **华为云平台：**云端平台结合天关上报的安全日志与取证数据，实现安全事件分析、防护策略的联动，为用户提供安全分析、事件闭环、安全预警、安全咨询等服务，其核心能力包括：

1. 接收天关防护节点上报的安全事件相关的关键信息，通过机器+人工的方式对安全事件进行分析，将准确的分析结果反馈给用户；
2. 对于授权云端自动处置的用户，提供安全事件自动闭环服务，将闭环策略直接下发到天关；对于未授权云端自动处置的用户，提供安全事件的处置建议，指导用户自主闭环安全事件；
3. 为用户提供周报、月报、紧急安全事件短信通知等服务，通过短信、邮件形式

为客户提供统一安全分析、专家服务、安全事件处置指导，使安全运维工作易懂、高效。



客户价值

华为乾坤安全云服务方案价值：

1. **降低部署门槛：**采用云服务的方式，可以根据用户业务场景，按需加载服务化特性，减少部署时间，安全能力快速交付，并持续运营保障提升防御效果；通过部署强大的安全解决方案和最佳实践，可帮助组织遵守严格的政府政策、保护客户数据并确保业务连续性，并将停机时间降至最低；
2. **个性化交付：**企业的规模、需求以及能力均不相同，安全服务可以根据组织的需求，提供定制化的服务，如安全服务能力、安全态势感知及安全事件通知等；
3. **防护持续升级：**通过客户样本数据不断提升服务能力和分析准确率，利用云端威胁信息、智能技术、大数据技术增强自动化威胁闭环处置能力，云端、本地实时升级，网络安全服务不断迭代，持续提升网络防御能力；
4. **加速威胁响应：**以服务化的方式提供代维、托管能力，可以快速发现威胁检测，并自动授权闭环，避免核心信息资产被盜、泄露；
5. **支持零信任可信接入：**通过对用户访问行为进行评估，识别风险行为，进行阻断或

重新确权，提升对混合办公、物联接入的访问行为管理能力，消减风险；

6. 智能防御体系：基于安全大数据驱动的智能防御技术将逐渐成熟，云服务可更便捷的引入算法，形成分析、管控、执行三层智能安全架构，全面覆盖云网边端。

目前华为乾坤安全云服务已经在超过10个行业客户部署超过10000套，提供便捷、有效的创新安全云服务，支持入侵监测、边界防护响

应、防勒索攻击、漏洞扫描、网络威胁评估、日志审计、威胁信息、紧急安全处置、安全月报、短信提醒等10多个安全服务，更加丰富的安全服务内容正在以按月迭代的方式上线。乾坤寓意天地，乾为天，代表华为云服务平台；坤为地，代表部署在本地的华为天关。通过创新的网络安全云服务，构建网络安全空间朗朗乾坤。



04

数据中心网络
正在向全以太网演进



 趋势

随着移动互联网、大数据、云计算、区块链相关应用的广泛部署，以及5G智能工控、HPC仿真验证、AI风控等强体验类应用在数据中心的兴起，数据中心已经成为数字经济时代流量和业务的制高点，基础设施即服务等各类技术创新与变革异常活跃。就服务对象而言，数据中心网络联接计算和存储服务器，承载服务器资源间的数据传输与交互，与计算和存储一起服务于云计算的各类上层应用。在这个交互链条中，云、计算、存储，任何一个服务对象的变化，都将触发数据中心网络的变革。

云的关键特征在于按需自助服务和资源弹性伸缩，开放的以太网可以很好地满足云业务诉求，可天然被云调用和管理，并具备良好的互通性、弹性、敏捷性以及多租户安全能力，当前已经成为通用计算网络的事实标准。而集中式存储以及高性能计算区域，传统网络采用较为封闭的FC以及InfiniBand技术。这些技术互通性与弹性不足且演进缓慢，无法匹配数据中心云化发展诉求。根据IDC数据，FC在数据中心市场规模仅为以太网的5%，IB则不到1%。随着以太网交换机发货量占比在数据中心持续稳健增长，FC和IB的市场逐步萎缩。数据中心中云计算技术的快速采用正在助长网络对以太

网交换需求的增长，智能无损以太网是当前以及未来的关键技术。

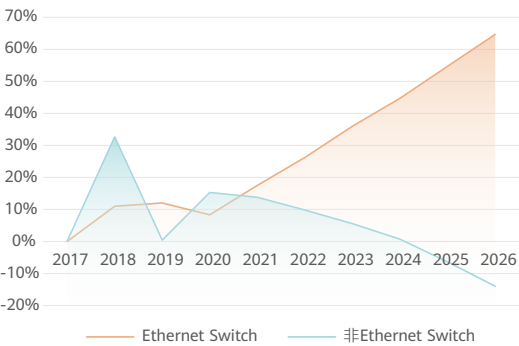


图7 IDC 2017-2026：数据中心以太网交换机和非以太网交换机发货增长率（含预测）

存储全闪存化驱动数据中心
以太化发展

数据激增和数据价值挖掘，催生了存储介质的革新，HDD迅速向SSD切换，SSD存储介质在短时间内将存储性能提升了近100倍，实现了跨越式的发展，而FC网络技术无论是从带宽或时延已成为存储网络场景的系统瓶颈，面临如下问题：

- 1. FC网络技术及互通性相对封闭，整体产业生态与连续性面临着很大挑战；
- 2. 产业规模受限，FC技术的发展相对迟缓，目前大规模商用带宽只有32G，存储业务开始呼唤更快、更高质量的网络；
- 3. 网络运维人员稀缺，能够运维FC网络的技术人员不足以太网维护人员的5%。这造成FC网络运维成本居高不下，故障解决效率低下。

计算单元从 PCIe 到以太提升性能

当前，占据数据中心服务器CPU市场绝对地位的Intel x86架构普遍使用PCIe 3.0，PCIe 3.0单通道仅支持8GT/s的传输速率，且通道扩展数量有限。在AI超算服务器已经全面迈入100GE网卡的时代，PCIe 3.0架构速率成为大吞吐高性能计算场景下的性能瓶颈。业界CPU/GPU厂商正在通过去PCIe总线突破总线的速率瓶颈，直接出以太网口来提供更高算力。



挑战

数据中心网络向全以太网化演进道路上面临三大挑战：

- 1. **网络丢包挑战：**业务数据激增，网络性能成为瓶颈，以太网天然有丢包，无法满足通信密集型HPC、高端存储等场景下极端性能要求；

- 2. **管理效率挑战：**近年来全球数据中心普遍采用集约化、规模化的建设原则，中小型数据中心被大型、超大型数据中心替代。数据中心网络管理规模快速扩张的同时，网络建设和变更依然依赖人工经验，业务规划人工梳理耗费数月，人工评审易出错，上线无校验，安装部署和联调需要2~4个月，超过85%的故障是靠业务投诉后才能发现。传统分散的多工具多平台的管理模式成为网络运维的效率瓶颈；

- 3. **多云多场景挑战：**一方面，为了满足核心业务稳定的同时快速响应变化，企业数据中心基础设施通常使用公有云-敏态业务与私有云-稳态业务双架构；另一方面，业务场景极大丰富，不仅行业间网络需求迥异，同一行业内不同业务场景下也有较大的不同。复杂的业务场景对网络的开放性和服务化能力提出更高的要求。



建议

采用融合以太网技术代替传统数据中心内烟囱式的三张物理网络，实现更大范围与丰富场景下的融合

随着数据中心全以太网技术的快速发展与成熟，传统数据中心内烟囱式的三张物理网络必将走向统一。推荐企业在下一代数据中心网络采用统一的以太网技术，突破一体机方案规模受限、管控割裂、厂商封闭以及场景适应性上的约束，实现更大范围与丰富场景下的融合。

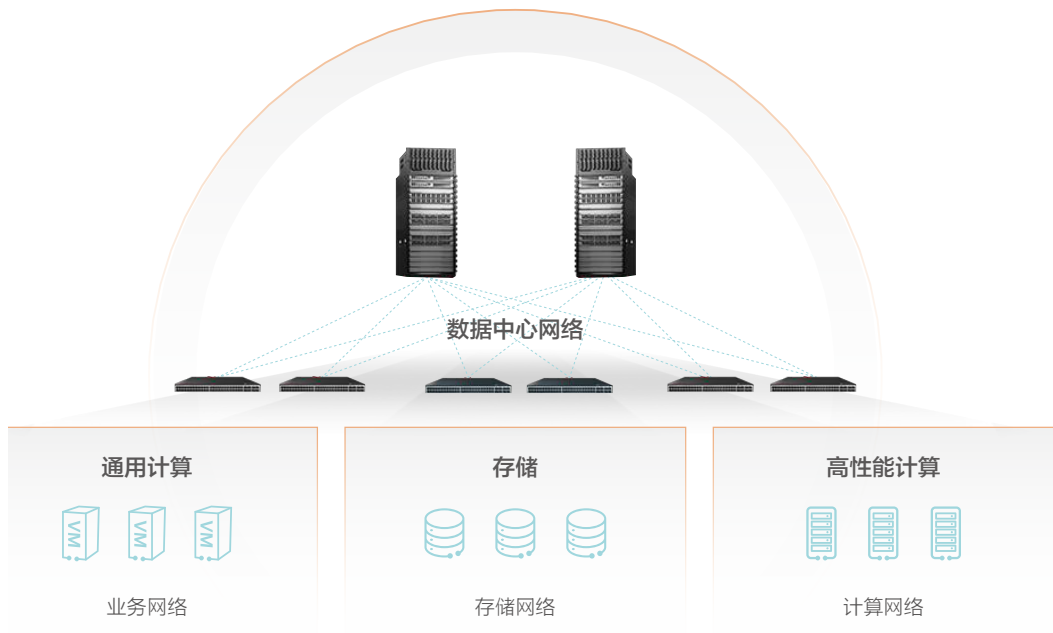


图8 数据中心全以太网架构图

- 1. **全无损以太网络，实现流量承载融合：**通用计算、存储、高性能计算网络统一承载在以太网技术栈上，组网协议统一，TCP、RoCE数据混流运行，打破传统分散架构限制；
- 2. **全生命周期自动管理，实现管控析融合：**基于统一网络数字孪生底座，加以大数据及AI手段，实现规划、建设、维护、优化全生命周期自动化，代替人工处理大量重复性、复杂性的操作，并基于海量数据提升网络预测和预防能力，打破多工具多平台分散管理限制；
- 3. **全场景服务化能力，实现全场景融合：**抽象数据中心网络“物理网络服务”、“逻辑网络服务”、“应用服务”、“互联服务”、“网络安全服务”、“分析服务”等核心服务能力，基于开放服务化架构实现多厂家、离线与在线数据的灵活接入。

满足多私有云、多公有云、混合云、以及丰富行业场景下的网络统一编排需求，支持算力跨云灵活智能调度，打破区域与场景限制。



解决方案

华为超融合数据中心网络解决方案：

华为超融合数据中心网络CloudFabric 3.0方案，核心部件包括CloudEngine数据中心交换机与iMaster NCE自动驾驶网络管理与控制系统，实现计算、存储、业务网络三网全IP架构，支持IPv6，并在业界率先实现L3.5自动驾驶网络能力，支持数据中心网络全生命周期自动化与全网智能运维，OPEX可降低30%，使能企业智能化升级。



图9 华为超融合数据中心网络解决方案3.0架构图



客户价值

华为超融合数据中心网络解决方案价值：

- 1. 全以太网HPC网络，100%释放算力：**传统以太网丢包带来性能瓶颈，0.1%的丢包会导致50%的算力损失。40多年来业界专家探索了很多路径解决以太网丢包，但无一例外都失败了：有通过流控反压来控制流量发送速度，但粗暴的反压机制会频繁停发报文，导致吞吐量极低；在网络应用流量越来越复杂的今天，控速时机也很难把握。华为创造性地将智能无损算法iLossless引入到网络联接中来，用算法代替专家经验实现实时精准控速，保证网络0丢包，实现规模不变，算力翻番；
- 2. 全以太网存储网络，存储性能提升93%：**对于存储网络，金融的双活数据中心场景性能要求最为严苛。同城数据中心之间的距离一般在30公里到70公里不等，由于长距光纤数据传输存在静态时延（5μs/公里），距离越长时延越大，与短距场景相比时延增长了百倍，流控复杂度指数级增加。为此，华为推出长距无损iLossless-DCI算法，在短距无损的基础上增加了距离变量，基于大数据分析提前应对流量变化，最大可实现200GE链路100公里无损传输，跨数据中心链路较FC网络可减少90%。在DC内和跨DC的同等距离场景下，IOPS较FC网络可提升93%，时延降低49%；

3. 运维管理全生命周期自动化，业务秒级部署与1-3-5故障处理：

针对业界SDN“设计校验靠人工，配置下发才自动”的半自动化运维模式，华为将数字孪生方法论引入网络管理领域，实现建全生命周期的自动化。基于网络数字建模，可综合评估400+影响网络设计的因子，可推荐最优网络设计方案并实现配置变更的秒级校验。基于网络知识图谱，可以实现故障1分钟感知，3分钟定位和5分钟修复。通过大数据挖掘与建模，识别网络对象与对象间的关联关系与故障扩散规律，感知90%潜在风险；

4. 多云多厂商异构统一管理，跨云业务部署从月到天：

多云场景下网络异构成为常态，多厂商设备往往配套多种控制器。一方面，当跨云业务变更时，需求要分解到多个控制器；如果控制器能力不满足，则需要依赖原厂商落入版本开发，周期在3~6个月不等。

另一方面，企业云管平台需要同时对接多个控制器，适配工作量巨大。南向和北向的多接口模式造成跨云网络部署动辄耗时数月，成为算力跨区流通的瓶颈。为此，华为定义统一的设备网元模型并构筑开放的南向框架，可实现跨厂商设备的统一管理以及设备驱动程序的动态加载。同时，CloudFabric 3.0北向可提供上千种丰富的网络API服务，实现云管平台侧灵活网络编排，业务上线周期从数月缩短至一周。

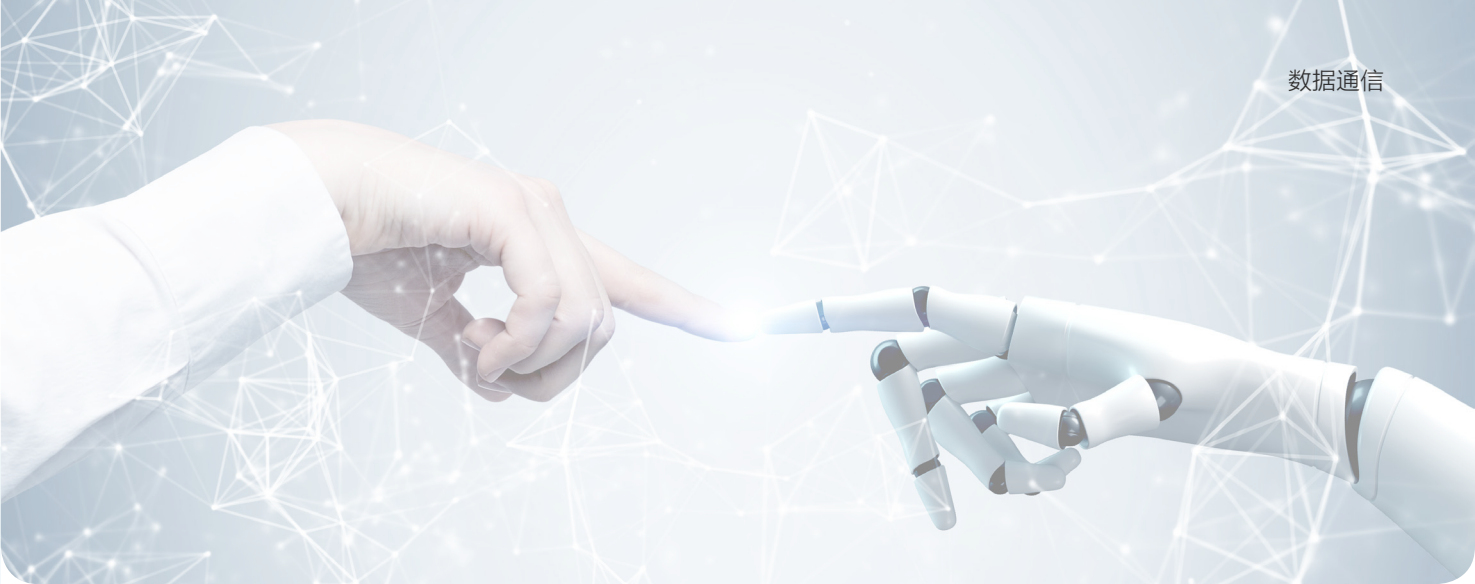
截止目前，华为数据中心网络已经在全球包括金融、政府、互联网、制造、能源等各大行业超过21000家客户的数据中心部署。展望未来，数字化快速发展驱动了网络的不断革新，华为将持续提升数据中心以太网络能力，充分释放算力，使能企业智能化升级。



05

基于人工智能的
超自动化正在改变网络
管理方式





趋势

在移动化、大数据、云计算、人工智能等新技术的推动下，企业的IT技术架构所涉及的网元数、技术栈、服务数等元素成倍剧增，而企业运维部门的人力却基本维持不变，这对网络运维带来了极大的压力，通常的情况是当业务出现波动后再从海量日志、监控数据中排查原因，往往已经造成难以弥补的损失，与此同时，新业务敏捷开通的诉求越来越强烈，为应对市场的竞争，企业往往需要基于市场变化，快速做出应对。过去以设备为中心的“救火式”运维，无法感知用户和业务体验，被动响应“故障”发生，难以满足数字化转型时代的用户和业务体验保障需求。



挑战

以设备为中心的运维模式痛点：

1. **以设备为中心，无法感知体验：**传统的网络管理是以设备为中心的，网管提供设备管理、拓扑管理、告警配置等功能，运维人员通过网管监控拓扑、告警来获知网络的异

常。然而，随着终端数量的增多、数字化业务的多样化，设备的正常运转已经无法代表用户和业务体验的正常。举例：AP 设备正常运转，但如果存在很强的同频干扰，将导致AP 服务的无线终端体验很差；网络设备正常运转，但如果存在 QoS 的配置错误，将导致某些应用的体验指标很差。

2. **被动响应“故障”发生，依赖现场定位和修复，故障恢复时间长：**网络运维人员，时刻等待着响应故障，尤其是一些重大活动、重大事件需要保障时。一旦出现故障，运维人员第一时间查看网络拓扑，命令行登录设备定位故障，60%以上的情景需要到达故障现场，针对已经消失的故障，需要等待故障复现或者尝试对故障进行复现。同时无线化进一步加剧了故障修复的复杂度，因为无线环境的复杂导致90%以上的问题需要现场定位。



从“以设备为中心”的运维理念，升级为“以数据为中心”的运维

相比传统运维方案，网络架构需要有如下变化：

1. 网络设备需要具备数据采集和一定边缘智能分析能力：

对于网络而言，人工智能只有基于价值数据挖掘才能真正发挥作用。过去，网络每天都会产生大量数据，海量的告警、日志一直困扰着企业运维人员，但是数据中的真正价值数据占比以及与业务的质量关联有限，即便应用最先进的人工智能算法，得到的信息对于业务价值也微乎其微。改变这种状态必须从数据源头入手，发掘价值数据来源是关键。因此网络设备需要支持实时地数据上报，同时能够在网元本地进行原始数据的初步分析，或者通过神经网络等矩阵运算算法实现计算加速，其核心目的是通过分布式的大量节点完成数据处理和分析，避免大量数据上送到管控中心，消耗计算能力；



2. 引入网络智能分析器基于大数据和 AI 的智能分析：

感知用户和应用的体验、发现故障/潜在故障和并识别根因，并将结果通过符合IT运维人员的工作思路，友好地展示出来。同时可以进行智能化的全局网络调优，支持智能化预测能力，实现网元级、业务级的资源预测，指导网络规划，具体特征如下：

1. 感知体验、对体验进行可视化管理：

- 对单个用户的 360°体验可视化和旅程回放；
- 对全局用户的体验可视化；

2. 主动识别用户和业务的体验问题，发现潜在故障并识别根因，最终给出修复建议甚至自动修复，而非被动响应：

- 故障发生，第一时间感知
- 识别出体验差的用户和应用
- 识别潜在问题，提前消除问题
- 对问题或故障，进行根因定位，给出修复建议甚至自动修复



华为智能原生数据通信网络

华为智能原生数据通信网络包括两部分：数据采集层和智能分析系统。

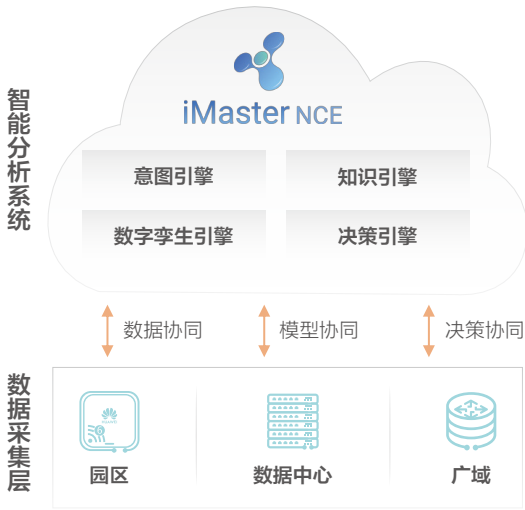


图10 华为智能原生数据通信网络架构图

1. 数据采集层：网络设备作为网络的触手，采集终端、设备和应用各个维度的指标和信息，包括终端接入的日志（包括协议交互）、终端性能指标、射频性能指标、设备性能指标、音视频业务性能指标等。传统网络管理系统采用 SNMP 来获取设备指标，但它有明显的缺陷，无法满足“以数

据为中心”运维理念需求。华为数据通信网络设备支持Streaming Telemetry技术，可以从设备上远程高速采集数据的网络监控，效率比 SNMP 效率高 20倍以上，可以实现 10 秒级的数据采集

2. 智能分析系统：网络分析器基于华为大数据平台构建，颠覆传统聚焦资源状态的监控方式，基于机器学习算法进行特征分析和基线运算，能够自动识别网络故障，故障定界以及自动网络调优等，并通过丰富的图形化界面对分析结果进行呈现，打造企业端到端的优质网络体验。

客户价值

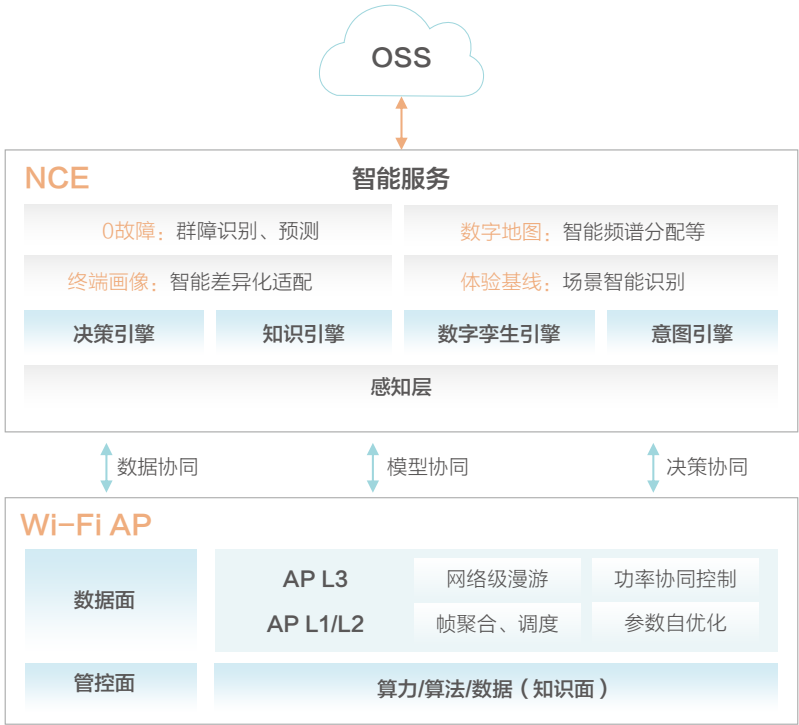
华为 IntelligentWAN 实现广域网智能原生



1. 多维度异常识别，网络健康可视：业务随流精准检测（iFIT），实现每业务每报文粒度的实时 SLA 感知，可以基于端到端和逐跳快速检测丢包、时延、抖动等业务质量。实现快速的定界定位。配置、告警、日志、KPI 多维海量数据上报，涵盖系统运行所有状态数据。80000 多项 KPI 监控指标，采用设备芯片 AI+NCE 在线学习协同技术，快速识别网络异常，捕捉静默故障，准确率达 90% 以上。
2. 基于 AI+ 知识图谱的智能故障诊断：结合华为运维部门多年故障诊断经验，累计 AI 训

- 练多达 2 亿个样本，涵盖 9 大类、200 多种故障根因分析，根因诊断准确率达到 99%。
3. 精准修复自愈闭环：对于 90% 以上常见故障提供精准故障修复建议，实现业务故障自愈同时保障 SLA 体验。自愈规则编排，完成运维流程自动闭环。

华为 IntelligentCampusNetwork
实现园区网智能原生



1. 网络健康度评估, 主动识别85%潜在网络故障
2. 用户体验全程可视，减少90%用户投诉
- 多维网络健康度评估：有线+无线网络健康度分析，定期报告推送；
 - 分钟级故障定界定位：主动识别 8 大类 200+ Issue，隐患问题提前预测
- 用户全旅程体验可视：每用户每时刻体验可视，故障可回溯
 - 接入问题协议级回放：快速定位用户接入问题，分析根因并提供修复建议

3. 应用体验保障，缩短95%问题定位时间

- 智能识别感知应用：AI 识别 1000+主流应用，主动识别应用质量
- 应用问题分钟级定位：独家随流检测技术，分钟级定界定位

- AI 漫游：基于不同终端类型建立漫游基线，差异化漫游引导，提升漫游成功率70%；

IntelligentFabric 实现数据中心网络智能原生

4. 智能无线调优，提升整网性能58%

- 预测性调优：预测 AP 负载，实现无线网络自动调优，整网性能提升 50%+；

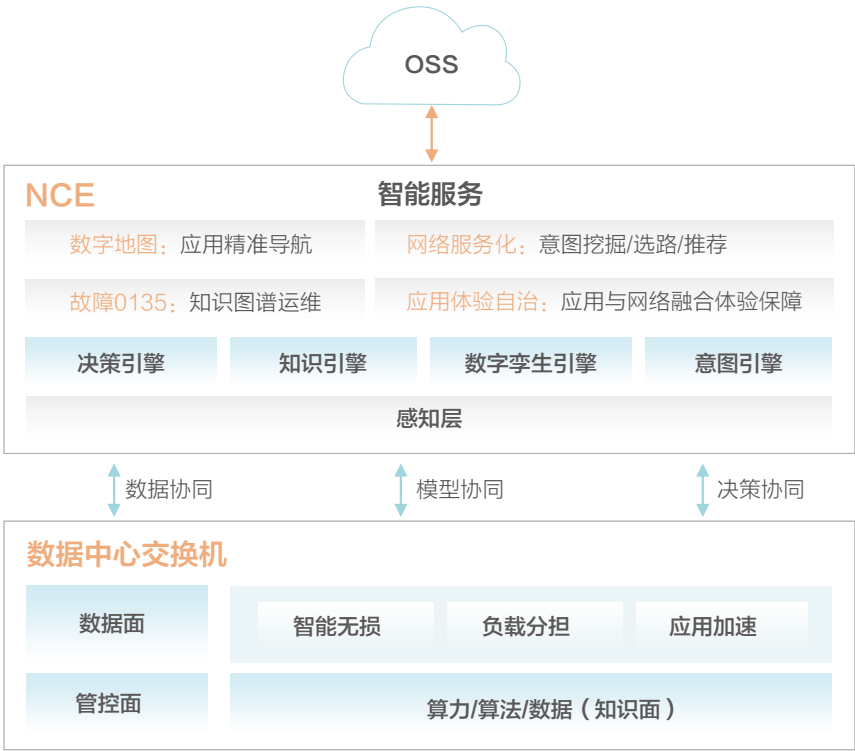


图11 华为IntelligentFabric智能原生数据中心网络解决方案价值

- **故障1-3-5处理：**iMaster NCE-FabricInsight 基于Telemetry技术实现对全网管理面、转发面和数据面全场景采集，异常问题1分钟感知；通过知识图谱实现3分钟自动推理故障及隐患根因，提供有效修复建议；同时可联动华为iMaster NCE-Fabric控制器，推荐优先故障处理预案，典型故障5分钟快速恢复。
- **网络意图验证：**iMaster NCE-FabricInsight 提供面向数据面的业务意图验证，在业务变更等重要业务保障场景7*24小时自动验证网络意图是否符合预期，自动识别全路径连通性，秒级感知业务及Underlay互通异常，针对异常路径可自动分析根因，及时通知用户闭环。

- **网络变更可视：**数据中心网络在运行期间，不可避免会涉及到网络变更操作，涉及上千条设备配置变化如何检测，单设备上万条表项是否能正常学习到，对于传统人工运维存在巨大挑战。iMaster NCE-FabricInsight提供网络快照管理，自动及手动同步设备配置、表项、拓扑、容量、性能五大维度网络快照，自动分析变更前后的差异，检测结果一目了然。
- **IP 360管理：**生产系统上云，VM部署和迁移由VMM自动完成，无法快速查找VM节点位置、何时迁移/下线、分布是否均匀等信息，网络侧被动运维。iMaster NCE-FabricInsight提供IP 360全景分析，快速了解当前在线VM数量和TOP接入VM交换机等

分布情况，帮助网络提前合理规划资源。如有异常，iMaster NCE-FabricInsight支持整网VM全生命周期管理，VM下线、迁移、上线记录实时可视，并提供整网IP快照分析，对比网络变更前后的所有IP变化，是否存在下线等异常。

- **全网日志智能分析：**网络故障后会产生大量日志信息，其中95%为无效日志，传统通过人工逐条排查，犹如大海捞针。iMaster NCE-FabricInsight支持全网日志事件可视，L0-L4多维度趋势、分布统计及详细信息一目了然；同时，支持异常日志降噪收敛，系统预置200+默认聚合、清除规则，也可人工自定义规则，提升日志分析效率。



06

工业网络走向
IT/OT 融合
使能工业智能化升级





趋势

工业控制走向远程集中化，工业智能化转型升级进程加速

1. 远程集控需求快速增长，助力现场少人化、无人化生产。传统工厂的工业生产控制室分三个层次，分别是现场的操作室、厂部的调度室、基地的总调度室，其中操作室处于生产一线的现场。化工、冶金等很多行业的现场操作环境恶劣，采用远程集中控制模式实现现场操作少人化、无人化，已经成为行业共识。
2. 数据无缝流转，工业智能化转型升级。利用网络信息技术和先进制造工具来提升生产流程的智能化，完成数据的跨系统流动，包括数据的采集、分析与优化，实现设备性能感知、过程优化和智能排产，是工业4.0智能化生产的基本要求。只有数据充分地采集、流转，并减少数据信息损失，才能真正发挥大数据的作用。同时，为了实现AI机器视觉质检、智能排产、过程优化，算力也需要能下沉到边缘甚至现场。“数据上得来、智能下得去”，随着工业智能逐步深入工业现场，控制和智能的融合、实时数据流和非实时数据流的融

合正在驱动工控系统向下一代智能工业控制架构发展。



挑战

传统工业网络面临新挑战

1. 现有的工业控制系统普遍采用工业以太、工业总线等局域网络架构，无法满足远程集控的诉求。以工业以太网为例，两个节点间最远距离为100米，超出100米将无法工作；这就无法满足大型企业的远程集控要求。采用光纤直驱的只能满足少数设备的远程控制要求，但对普遍的有大量控制设备的企业来说也不可行。在某钢企的某基地，需要将40km范围内的上千个被控设备的控制系统拉远到集控中心，如果采用光纤直驱的方式，需要部署上千对超过40km的光纤，这对企业来说是无法接受的。
2. 传统工业控制协议七国八制、互通困难，导致大量数据沉淀在各个碎片化、烟囱式的孤岛，难以开展大数据分析和闭环优

化，难以实现工业数据价值化，无法满足工业智能化演进需要。非标协议导致的大量数据孤岛。例如，传统的工业现场网络主要是采用现场总线或工业以太网技术，历史上各个行业的独立发展造成了多种各自不同的现场网络技术标准，如ProfiBus/ProfiNet、EtherCAT等，这些不同协议标准间难以互联互通。这些工业控制系统架构封闭，只能通过“外挂式”实现有限程度的局部智能，并不能满足智能制造的要求。

建议

打造先进工业网络，实现“数据上得来、智能下得去”，加速工业智能化转型

1. 设备网联化，综合运用Wi-Fi、物联网、5G、光纤等技术，提升工业人机物云的联网水平，实现数据的全面深度感知和无缝流通；面向柔性化制造对有线联网设备按需实施“剪辫子”改造，提升设备联网灵

活性，降低转线生产时产线调整的时间。

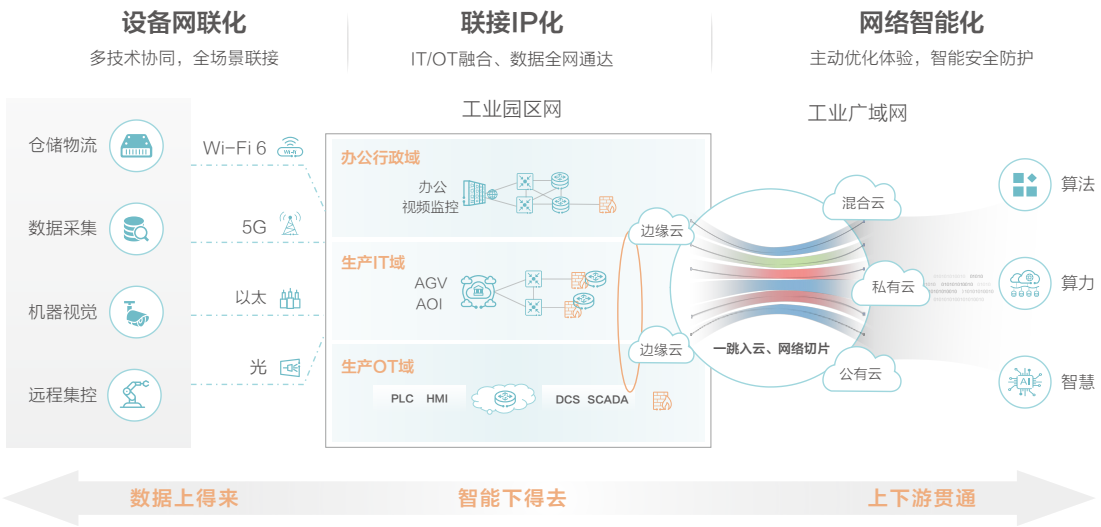
2. 联接IP化，引入“IPv6+”技术创新提升IP确定性服务能力，实现IT/OT融合。

“IPv6+”网络技术创新，特别是确定性IP技术，面向工业场景增强了IP网络的确定性服务能力，将推进工业网络IP化一网到底，助力全联接工厂建设和下一代智能工控系统发展，加速制造业数字化转型。

3. 网络智能化，提升网络面向不同业务的差异化服务和体验保障能力、面向海量物联终端的管理运维能力和面向安全威胁的智能防护能力，包括智能业务识别和体验保障、可信工业标识引入实现自动化可信入网、工业终端的AI指纹识别和网络行为智能管控、工业业务和网络的联动编排和主动优化、基于大数据的故障定界定位等。

解决方案

华为制造云网解决方案



1. Wi-Fi 6连续组网，稳定联接，物联融合

智能天线，网随人动，信号全场景覆盖零盲区，信号更强，速度更快；AI漫游，终端漫游不迷路，业务不中断；AI连续组网，感知整网质量，预知故障，自动优化

2. 工业级物联网关，边缘智能

丰富接口，工业级设计，适用多种物联场景；边缘智能，多容器管理，合作伙伴APP按需部署，实现工业协议IP转换；集成控制、管理、计算和通信等功能的基础开放平台

3. 统一承载，一网多用

- 网络切片，一网多用：层次化切片实现硬隔离，保证确定性带宽，切片规格高，支

持1000+切片；切片粒度精，支持10M粒度，资源不浪费

- SRv6一跳入云，支持确定性路径，网随云动，灵活调整接入多云
- DIP确定性低时延（低抖动），满足工业远程控制要求，经过产业链的共同努力

确定性IP技术已经取得了巨大突破，开始从技术原型走向商业创新。2021年，华为携手上海交大、宝信软件（600845）、紫金山实验室等合作伙伴完成全球首个广域云化PLC试验，在跨600公里距离的广域IP网络上实现了确定性网络服务，支持基于云化PLC的远程工业控制系统稳定运行。



07

联接无处不在
的算力和智慧生活



面向未来，网络既充满想象空间，也存在很多不确定性，需要全产业共同努力，共同探索这些新技术方向，迈向Net5.5G，打造无处不在的智能IP网络，联接无所不及的算力和智慧生活

面向2025年，数字化能力将持续改善每个人的生活与工作，数据通信网络作为数字化的底座，将数据和算力高质量的运送到个人与千行百业，激发数字活力，释放数字生产力。

联接个人：5.5G的发展将进一步带动沉浸式XR、千亿级移动物联、全息/触感互联等等新兴2C业务的兴起，极大丰富人们的数字生活，带宽诉求从1Gbps体验向10Gbps体验持续演进，抖动要从ms级降低至百us级，数通网络作为5.5G的承载底座，需要进一步提升带宽承载能力和确定性替换保障能力。

联接企业：千行百业数字化转型将进入深水区，一系列新的应用场景层出不穷，数字化智能化的能力将进一步赋能企业办公生产效率，进一步改善最终客户的服务体验，充分释放数字化生产力。一方面，企业联接的终端将更加丰富，NFC/BLE/WiFi/LoRA等越来越多制式的传感器、物联终端需要接入到网络。另一方面，AOI质检等数字化生产技术需要3.2Gbps/产线超高带宽；IP网络深入到OT场景使生产装备网联，这就对数通网络高带宽、确定性承载、泛在物联等能力提出新的诉求。而物联边界的扩展必然带来安全威胁的增大，扩大安全防护边界，提升安全防护效率也迫在眉睫。

联接算力：数据中心内部是算力产生环节。根

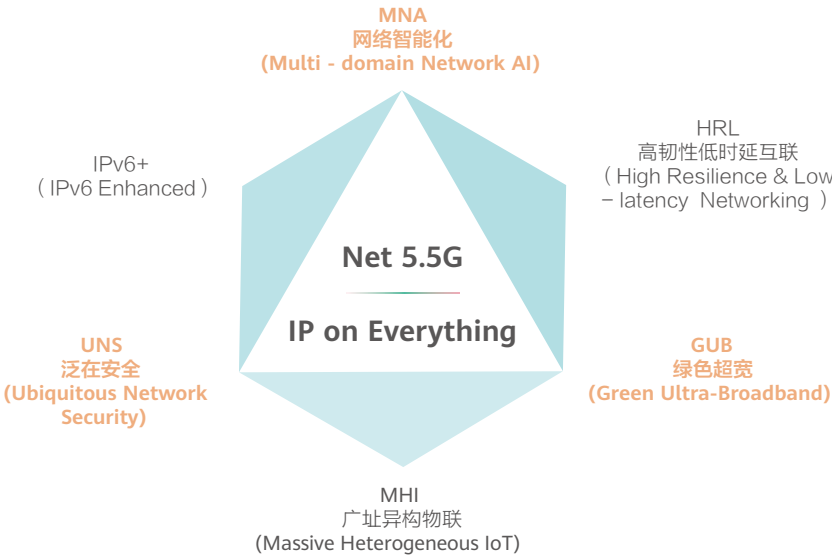
据IDC的预测，未来五年全球算力规模CAGR 50%，单中心算力从E级 -> 百E级演进，对接入带宽的要求也提升到了800GE。随着算力增长，单DCN的节点数量也相应增长，从十万级向百万级演进，需要DCN能够满足超大规模组网诉求。大流占据带宽大，网络极易负载不均，根据Google和鹏城实验室数据，当前AI计算的DC有效吞吐率<25%。均衡数据流调度，提升有效吞吐率也成为关键问题。DCN以太网络深入到服务器内部，全以太网总线互联逐渐成为业界共识，intel等计算芯片头部公司在高速互联选择了XPU直出以太技术方向。为此，对CPU/GPU/内存超低时延互联提出挑战。

对于算力的运输环节，也存在着新的场景与变化。首先，多云多算力已经成为必然趋势。Flexera《2021云状态报告》显示，采用多云的企业占比92%，受访者平均使用2.6个公有云和2.7个私有云，而且算力使用也趋向多样化，生产执行系统MES、视频协作等业务系统倾向通用算力；新车研发、风阻/碰撞实验等模拟类需要超强算力，一般使用HPC算力；产线质检、自动驾驶训练等则倾向使用AI算力；为此，多样化分布式算力促进一网多云灵活互联；AI和HPC数据量大，单次传输量10T/100T，加速承载网络带宽进一步提升。

AI算力深入到企业生产环节，工业运动控制等要求抖动10us级。

针对这些新的诉求与挑战，Net5.5G以端到端SRv6为关键的技术特征，并在六个方面进行

加强与定义：绿色超宽、广址异构互联、高可靠低时延互联、IPv6+、网络智能化与泛在安全。持续提升IP网络能力，打造高质量数字化底座，联接无处不在的算力和智慧生活。



1. 绿色超宽:

带宽是各种数字应用发展的基础。现在8K视频的带宽要求在100Mbps以上，移动Cloud VR要求230Mbps。与此同时，各种人工智能的应用也在蓬勃发展。人工智能训练所用数据集的规模也在不断增大，从T级扩展到10T、甚至百T。我们曾与中国移动在网络自动驾驶方面进行过联合创新，40T的训练数据通过70Mbps的专线传输到数据中心，耗时7天。因此，显然需要更大的带宽，而且是可以需动态调整的带宽才能支撑这些新业务的发展。迈向未来，越来越多的优质服务将不断涌现。沉浸式XR、全息通信等都是消耗带宽的应用程序。单路沉浸式XR的带宽将达到4.4Gbps、高保真移动全息图像的带宽将达到10Gbps，构建数字孪生体验的全息通信甚至能达到Tbps。

我们预计网络流量将保持每年30%的增长速

度，网络带宽实现3年翻番、10年10倍增长。网络端口速率将从现在的100G为主升级为400G、800G的时代；与此同时，相关的硬件和芯片底层技术也将出现突破性的发展：芯片架构从当前2D/2.5D Chiplet架构向3D Chiplet演进的同时，融合异构NP处理器架构实现DCN交换机与路由器向800GE端口演进。硬件散热技术会从当前设备级的风冷和液冷，向芯片级的射流冷却以及硅基微液冷发展，同时还会出现更为先进的热界面材料，导热系数提升一个数量级（10倍）。无线侧，Wi-Fi的带宽将以更快的速度发展，基于AP协同算法及D-MIMO增强，Wi-Fi 7峰值带宽将能够达到30Gbps。

2. 网络智能化

面向未来，网络复杂度将面临更大的挑战：5G、5.5G、X2B等业务规模部署，网络规模10倍增长；对标云服务，云、网一致体验，网络

服务化、体验电商化带来10倍体验要求；天级业务敏捷开通，分钟级故障自修复，客户零投诉，网络运维提出10倍的效率要求。

应对上述挑战，我们定义网络要逐步实现自动化自治：网络数字地图，像Google Map一样，数字地图是在线网络规划的基础。实时感知，多维度感知，毫秒级实时感知构建网络数字地图，支持网络路径自动化精准导航，精准扩容；网络智能分析仿真，基于数字孪生构建网络仿真拓扑，搭建网络配置理想库，现实库，支持基于理想库的网络规划部署和变更仿真。支持100K节点大规模网络，配置面、数据面仿真，形式化快速仿真算法，确保准确无误后，再部署到现实网络，避免网络配置变更导致的人因差错；知识图谱，基于知识图谱自主学习不断丰富故障知识库，实现故障处理自动化，告警自动降噪，3分钟故障根因自动聚合分析，5分钟自动识别影响的业务；AIOPS，云端AI、网络级AI叠加网元AI，自动训练，自我成长，自主决策，实现智能运维闭环。AI算子快速编排，开放可编程的路径计算，业务流质量劣化、网络拥堵自动优化，故障驱动Runbook自动化修复。

3. IPv6+

新兴业务、应用、场景带来的数据量持续增长，各行各业对算力和网络提出了迫切的需求。算力已经成为新的资源形态，和电力一样无处不在。网络需要让算力更易泛在扩展，让数据更易流动，用户更加便捷使用。IP网络需要提供新的协议设计，实现算力和网络资源的统一编排，实现网络感知算力进行更优的调度，实现无拥塞、低时延的网络差异化承载。

目前网络仍然无法感知应用，只能通过不断增加带宽由轻载来换取业务的质量保证。然而随

着边际效应的逐渐消失，运营商的不断投资并没有带来相应的增益。

APN6充分利用IPv6/SRV6的可编程空间，将应用信息（ID、SLA需求）携带入网，突破应用与网络边界，再加上10K级超大规模的切片技术，使得网络能够为应用提供精细化运营，实现应用级的业务导流、以及差异化SLA保证。同时，应用侧云化资源与承载网络可以进行信息交互通告，通过引入CFN算力路由，实现云网资源统一调度以匹配新业务需求。为了能够更好地实现云网一体化调度，SRv6等创新技术将不再仅仅局限在广域网络使用，它要进一步延伸到数据中心内部直达ELB，实现SRv6入云。

4. 广址异构互联

数字化发展，一方面需要通过云使能的数据服务对业务进行赋能，另一方面一方面我们需要将数据的触点全面渗透到在办公、生活、生产的各个环节。经过了20多年的发展，物联网已经从面向采集的非关键业务走向面向控制的关键业务，需要高带宽，高密度覆盖、低时延的物联网网络。

面向未来，我们希望可以在不改变现有单对双绞线情况下，引入NG-SPE一线多频和OFDM调制技术，从当前的100K能力升级到10M的带宽能力，实现100倍的带宽提升，满足各种现场视频的回传，部署成本降低50%；其次在Wi-Fi接入领域，NFC / BLE / WiFi / LoRA共基带融合接入技术，能够实现通过AP连接各种制式的终端和传感器，降低复杂度和成本，接入密度从1K/1000m² 提升至100K/1000m²，接入带宽从Kbps提升到Mbps。

5. 高韧性低时延互联

到2030年，通用算力增长10倍到3.3ZFLOPS，AI算力增长500倍到105ZFLOPS；全球每年产生数据量增长23倍到1YB。数据中心规模百倍增长。未来极致沉浸式体验需要网络端到端保障“头动至显示”（MTP）小于10ms时延，逼近人类感知极限，避免晕眩；远程手术，以1米/秒的速度移动，控制精度在5毫米，总延迟要小于5毫秒，且需要99.9999%以上的可靠性；越来越多的新兴业务需要网络具备确定性体验保障能力。

大规模组网：创新的Dragonfly+直连拓扑，保证任意服务器之间跳数相等，时延确定，避免传统Spine-leaf架构带来的调度不均衡，导致算力损失的问题。自适应路由技术降低30%时延，故障收敛速度从100ms降至100ns。实现M级算力池规模，ns级故障收敛。同时引入网络级均衡算法，对DCN内流量进行统一调度分流，保障DCN内流量均衡，吞吐率提升至90%以上。

原生SLA支持的新型QoS架构：现有的QoS调度架构，都是基于队列优先级调度的，高优先级的队列能优先获得调度转发，主要是解决共享资源的分配问题，并不对服务的质量结果负责，在SLA保证，尤其是时延保证方面，存在局限性。新型QoS架构，与现有基于优先级调度的方式不同，将直接以时延、带宽、丢包率等维度，实现面向SLA的精确量化调度。借助ML能力，实时学习/预测网络流量特征，通过AI推理，动态自适应的调用新型QoS架构能力来实现最优化的队列调度，达成SLA目标。

确定性IP新协议：面向广域网络场景，IP网络中源和宿之间存在多种可达路径，众多节点参与，确定性IP协议需要具备SLA约束的拓扑路径选择、节点QoS队列的分配，并结合网络负载等多制约因素下的最佳路由与资源编排；未

来多感官应用体验、分布式ML、多方协作应用等会产生多数据流连接间的同步协作，确定性IP需要具备面向应用/任务的多连接确定性协同保障能力，达成应用/任务的整体QoS目标。

TSN2.0确定性承载：面向生产园区内部网络，TSN技术进一步发展，通过引入门控队列调度、免时钟同步、大规模网络编排等能力，可以将时延从10ms降低至100us，1K网元/10K流实现分钟级编排，满足数字化生产需要。

以用户为中心的网络切片：网络切片是未来用户网络数字空间的重要承载方式之一，以用户为中心构建IP网络切片是未来的重要演进趋势，将由当前面向连接的资源切片向包括链路安全、算力服务、数据存储等新型网络服务切片转变，具备按需、灵活的定制；具备移动性，实时弹性的切片管控，实现切片随行。

6. 泛在安全

随着万物互联、云原生，元宇宙的发展，物理世界与数字世界在不断发展演进融合，网络边界不断延伸，一方面安全边界和暴露面急剧扩大，另一方面业务的安全需求也开始呈现多样化，动态化、普惠化的特点。传统的外挂式的安全防护体系不适用未来网络的安全诉求。未来，“安全”将作为一种架构属性融合进未来的网络中；基于智能的自动化安全运营也会逐步替代人类分析师；安全将成为水、电、算力类的基础服务随着网络延伸按需提供。

智能化安全防护技术被网络安全领域普遍应用，用于提升安全防护的效率和效果，同时大幅降低成本，主要有以下几个方面：通过智能漏洞挖掘、漏洞利用技术、持续防护有效性评估等，实现风险识别率100%；基于指令模拟高对抗样本检测技术，新型APT攻击检测率高

达99%；基于亿级恶意样本家族知识图谱和分布式AI本地自学习，实现本地自主研判、闭环处置比例达到80%；基于网络安全数字地图和统一安全编排总线，通过Playbook模板自动推荐和安全语义机协同，实现狩猎调查自动化，提升效率6倍。通过联邦学习、差分隐私和AI本地训练，降低威胁分析的传输、存储成本50%，同时通过分布式AI硬件加速，实现5

倍算力提升，安全防御总成本降低70%。

面向未来，网络既充满想象空间，也存在很多不确定性，需要全产业共同努力，共同探索这些新技术方向，迈向Net5.5G，打造无处不在的智能IP网络，联接无所不及的算力和智慧生活。



华为技术有限公司
 深圳市龙岗区坂田华为基地
 电话: (0755) 28780808
 邮编: 518129
www.huawei.com



商标声明
 华为 HUAWEI，HUAWEI，是华为技术有限公司的商标或者注册商标，在本手册中以及本手册描述的产品中，出现的其他商标、产品名称、服务名称以及公司名称，由其各自的所有人拥有。

免责声明
 本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺，华为不对您在本文档基础上做出的任何行为承担责任。华为可能不经通知修改上述信息，恕不另行通知。

版权所有 © 华为技术有限公司 2022。保留一切权利。
 非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。

东西智库 | 专注中国制造业高质量发展

东西智库，专注于中国制造业高质量发展研究，主要涵盖新一代信息技术、数控机床和机器人、航空航天、船舶与海工、轨道交通、节能与新能源汽车、电力装备、农机装备、新材料、医疗器械等制造强国战略十大领域，并提供战略咨询、规划编制、项目咨询、产业情报、品牌宣传等服务。

欢迎加入东西智库小密圈，阅览更多制造业精选信息

 知识星球

微信扫码加入星球小密圈

交流 | 分享 | 研究

赠**1万+**制造业精选资料

