星河AI 网行天下

HUAWEI

华为星河AI
金融目标网络白皮书

高阶智能　超高韧性　敏捷高效　安全可信　极致体验

编委会

版权声明

序言

如今，我们已经站在第五次工业革命的门槛上，不同于之前的任何一次工业革命，第五次工业革命以5G、云、AI为代表的数字技术正不断突破边界，实现跨越式发展，一个波澜壮阔的智能世界正在加速到来。

华为预测，到2030年，全球联接总量将突破2000亿，全球通用计算算力将达到3.3 ZFLOPS (FP32)，AI计算算力将超过105 ZFLOPS (FP16)，增长500倍。算力 = 单芯片算力 × 集群规模 × 算力效率 × 算力可用率，网络则是将算力有机联接起来的智能世界的基石，网络的使命就是提升算力效率和算力可用率，从而最大程度释放算力并灵活输送算力。

金融行业正逐步进入Bank 5.0智能化时代，用AI激活金融创新、风险管理、投资管理、交易监管、客户服务等方面的巨大潜力，这需要不断攀升的海量算力以及新一代网络作为业务底座。在数据中心，一网承载通算、智算和存储，通过提供高运力网络赋能金融大模型训练和推理。在广域，网络需实现弹性超宽，把AI算力高效可靠地输送到各级金融机构和网点。在园区，要实现一网多用，保障算力随时随需获取和VIP金融业务的极致办公体验。在网络安全，需保障各级金融机构数据和算力流转的极高安全。新一代金融网络的核心是在规、建、维、优生命周期内全面智能化，从而进一步激活金融业务的智能化。

基于上述使命，华为打造了面向智能时代的新一代金融网络—**华为星河AI金融网络**。如同星河联接无数繁星，组成浩瀚宇宙，星河AI网络智联万物，充分释放智能和算力，加速金融行业智能化转型，跃升数智生产力。

华为数据通信产品线
政企领域总裁

目录

1 金融数字化和智能化演进对网络的诉求 01

2 高阶智能，加速金融行业迈向Bank 5.0 03

2.1 星河AI智算网络，释放金融AI训练海量算力 03

2.1.1 金融行业AI大模型应用正走深向实 03

2.1.2 金融智算网络需要大规模、零丢包、高吞吐、全自智 04

2.1.3 星河AI金融智算网络方案释放AI时代高算力 04

2.1.4 成功案例：星河AI金融智算网络助力某客户大模型训练性能提升16%~23% 06

2.2 AI赋能网络，打造智慧金融基础设施 07

2.2.1 黑科技1：NetMaster网络大模型，让运维更智能 07

2.2.2 黑科技2：智能未知威胁检测，让数据更安全 07

2.2.3 黑科技3：Wi-Fi 7动态变焦天线AI智能漫游，让体验更流畅 08

2.2.4 黑科技4：AI算法与架构双创新，让投资更绿色 08

3 超高韧性，助力金融容灾无忧，业务永续 09

3.1 金融安全规范对数据中心网络的可靠性提出更高的要求 09

3.2 传统金融网络存在容灾能力弱、可靠性可用性不足等问题 10

3.3 星河AI金融数据中心网络方案，极大提升网络容灾能力和可靠可用性 10

3.4 成功案例：华为助力Z银行构筑敏捷弹性、高可用的新一代云数据中心网络 12

4 敏捷高效，实现网络自动驾驶 13

4.1 网络数字地图助力金融产品敏捷开发，提升金融业务上线效率 13

4.1.1 金融业务的快速迭代，对网络运营提出了更高要求 13

4.1.2 越来越频繁的网络变更，网络运维判不准、看不全、看不清、耗时长 13

4.1.3 华为率先在业界推出网络数字地图，推进金融网络运维智能化 14

4.1.4 成功案例：华为网络数字地图助力X银行网络拓扑准确率99%，业务上线时间从周缩短到天 15

4.2 金融广域网络“IPv6+”全面部署，保障金融客户多地多中心灵活高效互联 16

4.2.1 金融业务数字化高速发展，对广域网络服务质量提出了更高要求 16
4.2.2 传统金融广域网面临着扩容成本高和部署慢的问题 17
4.2.3 华为“IPv6+”智能云网方案实现多地多活云网协同、智能调优和差异化服务 18
4.2.4 成功案例：华为SRv6智能调优方案，助力Y银行带宽利用率提升20% 19

5 安全可信，保障金融业务安全 21

5.1 金融智能安全防勒索，多层防护构筑坚固堡垒 21
5.1.1 勒索攻击愈发频繁，金融业务长时间中断风险激增 21
5.1.2 勒索病毒千变万化，传统网络安全面临新挑战 21
5.1.3 华为安全防勒索技术，构建基于完整攻击链的全网防护体系 22
5.1.4 成功案例：华为构建领先的多层保障体系，打造安全运营环境 23
5.2 金融终端安全无感接入，防仿冒防私接 23
5.2.1 各类物联终端广泛应用，提升金融业务效率的同时，带来安全隐患 23
5.2.2 海量终端联网，对网络安全提出更大挑战 24
5.2.3 华为终端安全无感接入技术，实现终端防仿冒、网络防私接 24
5.2.4 成功案例：私接秒级检测与阻断，保障金融网络安全 26

6 极致体验，打造场景化智能网点 27

6.1 金融服务嵌入到日常生活中，金融网点加速场景化转型 27
6.2 海量智能设备引入，对业务体验和连接安全带来新的挑战 27
6.3 华为Wi-Fi 7和SD-WAN，支持终端高密安全接入、分支灵活互联、业务体验保障 28
6.4 成功案例：华为高品质园区和智能SD-WAN方案，助力A银行打造面向数字时代的智慧网点 30

7 写在最后 31

01 金融数字化和智能化演进对网络的诉求

银行数字化在经历了Bank1.0到Bank4.0之后，开启了向智能化演进的Bank5.0时代。第一个波次（Bank 1.0到Bank 3.0）聚焦提供线上线下一体化、实时稳定的金融服务；第二个波次（Bank 4.0）聚焦构建平台+全场景生态的商业模式，银行重构其现有业务变得更开放，与生态伙伴的服务紧密结合；第三个波次（Bank 5.0）聚焦重新定义个性化产品和服务，优化运营效率，制定更精准的投资策略。在整个业务流程里深度应用大数据和人工智能，如下图所示。三个波次在并行演进，以AI为标志的智能化对金融业注入了强劲的创新力，不仅提升了银行的竞争力，也为客户提供了更优质的金融服务，驱动了整个金融生态系统的变革。

AI大模型加速重构金融科技与服务模式，迈向智能化时代

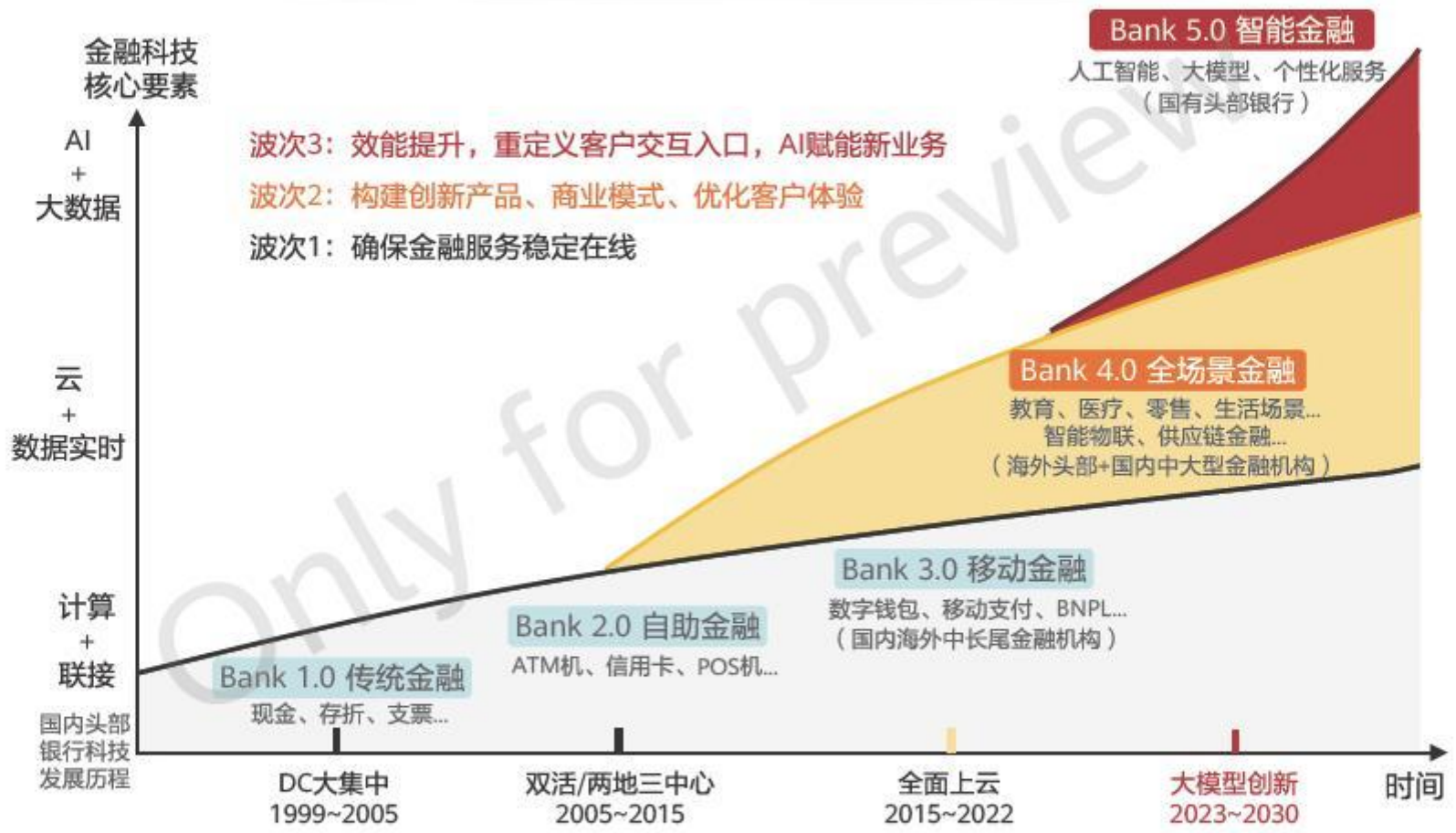


图1-1 银行业科技发展历程的三个波次在并行演进

智能化转型深层次驱动力是银行如何更好、更高效地服务客户，更快地推出新产品和管理风险，转型成以客户为中心的数字化经营、平台+生态的商业模式。数字化经营的银行通常将**月活跃用户（MAU）和日活跃用户（DAU）指标设定为关键KPI**，数字化分析用户行为，不断提升用户体验；通过实时数据采集和分析进一步反哺业务产品设计，**数据成为经营决策的主要依据**；AI也逐渐从客户服务等辅助领域进入到到营销、风控等核心业务领域。

伴随着银行的智能化转型，IT投资方向也发生了变化，Run the Bank（维持基本面，保持银行运行）的投资在逐渐减少，越来越多地投向Transform the Bank，提升智能化水平（也称Change the Bank，以云、大数据、AI等新技术再造IT系统）。对外服务的业务部门更加聚焦用户体验，对内服务的科技部门构建起各类能力平台，并将组织的能力沉淀在这些平台上，使得全行的业务、科技、运营等各部门能够便捷、高效、自主地使用这些能力。在这个过程中，科技部门从以往被动响应业务需求的角色，逐渐转向主动驱动整个转型过程。

在银行的上述转型过程中，业务韧性无比重要，关注单个系统的韧性转变为关注用户旅程韧性，韧性必须被重塑。金融机构需要具备稳健韧性的数字基础设施、敏捷弹性的平台能力，可迅速迭代金融产品，提供安全可靠的持续服务，以应对用户需求的日新月异。

华为提出了金融韧性基础设施目标架构“4 Zeros”，包括：Zero Downtime高可用、Zero Wait极致体验、Zero Touch高效运维和Zero Trust可信安全。这四个“Zeros”不是割裂的能力，而是需要云、数据库、数据中心、广域网络和分支网点，云网存算跨域协同，形成端到端的韧性体系。网络是连接韧性技术设施各组件的核心枢纽，我们认为金融目标网络演进架构为：**高阶智能、超高韧性、敏捷高效、安全可信、极致体验。**

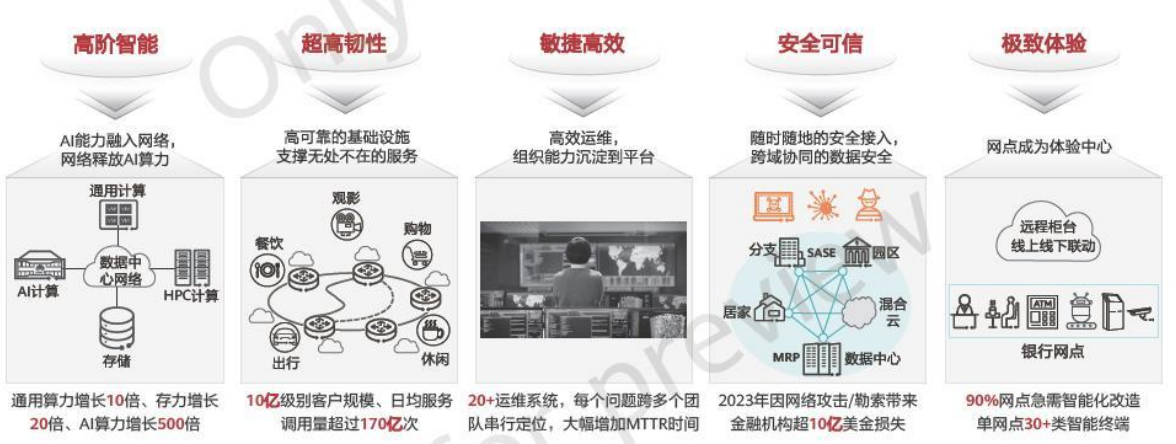


图1-2 金融目标网络需满足“高阶智能、敏捷高效、安全可信、超高韧性、极致体验”五个演进目标

02 高阶智能，加速金融行业迈向 Bank 5.0

2.1 星河AI智算网络，释放金融AI训练海量算力

2.1.1 金融行业AI大模型应用正走深向实

ChatGPT引爆人工智能产业，金融行业进入了生成式人工智能时代，AI训练模型正在从万千小模型走向百模千态的大模型。金融业是数据密集型、知识密集型行业，同时又是科技驱动型行业，具备良好的数字化基础，是大模型应用落地的最优行业之一。金融业务要提供更加便捷、快速、安全的服务体验，最重要的措施之一是运营智能化，也就是将AI能力与金融业务场景深度结合。

当前，金融行业大模型的发展正在跨越拐点，从“预测推断”走向“内容生成”，在金融创新、风险管理、投资管理、交易监管、客户服务等方向发展迅速。

图2-1 金融AI模型场景举例

为了吸纳海量的知识和业务数据、适配复杂的业务场景，金融大模型的参数量节节攀升，随之而来的是对算力的蓬勃需求，这使得金融智算中心AI服务器规模不断增长，正从千卡走向万卡。

2.1.2 金融智算网络需要大规模、零丢包、高吞吐、全自智

与基于TCP/IP的通算网络不同，AI智算网络使用RoCE，接入带宽高达200GE/400GE甚至更高。网络万分之一的丢包，算力变九成，千分之一的丢包，算力变七成。因此金融智算网络必须独立建网，其核心要求是：大规模、零丢包、高吞吐、全自智。

» **挑战1-规模不足：现有智算网络架构复杂，建网成本高，扩展性不足，导致算力受制约**

智算网络作为智算中心的骨架，一方面要适配AI集群规模，另一方面需要平衡成本、效率、可扩展性。某智算组网方案，在400GE集群规模大于2048卡时，需要3层组网，拉高了建网成本，增加运维复杂度。另一种2层架构方案，最大只支持4000张算卡互联，无法规模升级和演进，算力受到制约。金融智算网络既要架构极简，又要可持续向万卡演进。

» **挑战2-吞吐不足：网络负载不均，整网吞吐不足50%，算力无法充分释放**

金融AI训练过程中，网络流量的特点是：周期性、单流带宽大、流数量少，整体训练性能受限于最慢的流。传统的网络负载均衡基于逐流Hash，在AI训练时极易出现Hash不均，既有的链路满吞吐甚至拥塞丢包，有的链路却空闲，而0.1%的丢包会造成AI训练吞吐下降50%，导致AI训练时长超预期，付出更多训练资源成本和时间成本。

» **挑战3-部署能力不足：网络部署效率低，开局耗时上月，导致金融AI应用上线晚**

智算网络规模随算力集群规模不断增长，导致网络部署难度大、效率低、易出错。以千卡集群为例，几十台接入交换机需人工逐台手动配置，还需与计算、存储系统进行多项参数的反复对接联调，部署至少耗时一个月。平均6‰的连线错误和人工排查又进一步延长了部署时间。网络部署效率低，导致AI训练启动时间晚，不利于金融AI应用的敏捷上线。

» **挑战4-可靠性不足：网络故障定位时间长，导致AI训练迭代过程有40%时间被迫中断**

AI训练系统涉及计算、网络、存储的软硬件之间的复杂交互，训练过程中极易出现各类异常，导致训练频繁中断。某大行的某次AI集群训练时长90天，期间出现110+次故障，其中网络故障25次，占比达到22%。网络出现故障后，只能通过二分法排查，一排查就浪费半天，在此期间计算集群无法正常工作，导致AI训练迭代过程有40%时间被迫中断等待。

2.1.3 星河AI金融智算网络方案释放AI时代高算力

华为星河AI金融智算网络方案，以网强算，为金融客户搭建极简无损高吞吐的智算网络，充分释放AI时代高算力。

» **价值1-极简网络架构平滑扩展到万卡，减少30%网络端口，部署成本低**

金融行业AI集群规模正从千卡走向万卡，因此金融智算网络可平滑扩容须作为金融智算网络的建网标准之一。

华为星河AI金融智算网络方案提供极简的2级架构组网方案，支撑千卡、万卡集群，且从千卡扩容到万卡过程中无需改动网络架构，可实现按需灵活扩容。当集群规模大于2048卡时，与业界传统的3级网络架构相比，可减少30%的网络端口，建网成本更低。极简的2级架构也更利于提升部署和运维效率。

组网方式	规模	性能	组网成本：交换机接口	组网成本：光模块
华为框盒2级组网	8K*400G / 16K*200G	满吞吐	24K*400G	16K*400G + 8K DAC
业界盒盒3级组网		20%-50%有效吞吐	40K*400G	40K*400G + 16K*200G

图2-2 华为极简2级组网与业界3级组网对比

» **价值2-华为创新的网络级负载均衡技术NSLB，整网吞吐从50%提升至95%，金融AI训练效率整体提升10%**

智算网络吞吐量直接影响算力效率，因此金融智算网络吞吐量达到90%以上必须作为建网标准之一。华为创新的网络级负载均衡技术NSLB（NSLB-CP、NSLB-DP、NSLB-gAR等）面向AI训练场景量身打造。根据AI训练的流量特征，将搜集到的整网信息作为创新算路算法的输入，从而得到更优的流量转发路径，整网吞吐从50%提升至95%，金融AI训练效率整体提升10%。

AI 模型训练测试场景（华为星河AI网络 vs. 传统以太数据中心网络）*

模型	华为	传统以太网（ECMP 等价路由负载分担）	华为较传统以太性能优势
HCCL (Huawei Collective Communication Library) All_Reduce 最大带宽	38.5GB/s	24GB/s	**60%**
BLOOM (BigScience Large Open-science Open-access Multilingual Language Model) 每秒样本数	59.5	50.7	**17%**
VGG16 每秒识别图像数	13,998	11,394	**23%**
LLaMA (Large Language Model Meta AI) 每秒样本数	22.5	17.1	**32%**

带宽测试（华为星河AI网络 vs. 传统以太数据中心网络）*

模型	华为	传统以太网（ECMP 等价路由负载分担）
Perftest ib_write_bw 带宽测试中各Leaf交换机端口出方向平均占用率	**98.9%**	59%

* 以上数据均来源于Tolly测试报告《AI模型训练性能 华为星河AI网络 vs. 传统以太数据中心网络》（#223143ZH）

图2-3 华为星河AI网络与传统以太数据中心网络部分对比测试数据

» **价值3-计算网络一体部署，万卡集群1周交付，参数调优从20天缩短到1天**

算卡规模越大，网络部署的工作量就越大。某两千卡规模项目历时2个多月才完成上线，其中仅配置问题定位就花了两周。因此金融智算网络支持与计算自动化联调须作为金融智算网络的建网标准之一。

华为通过统一规划工具完成计算和网络的参数规划，并分别由计算管理工具和网络控制器iMaster NCE下发计算和网络配置，保证端到端规划与配置的一致性。同时iMaster NCE具备参数仿真校验、自动排查线路错误等功能，确保网络配置的正确性。某千卡大模型项目，使用华为方案仅一周就完成了网络配置。

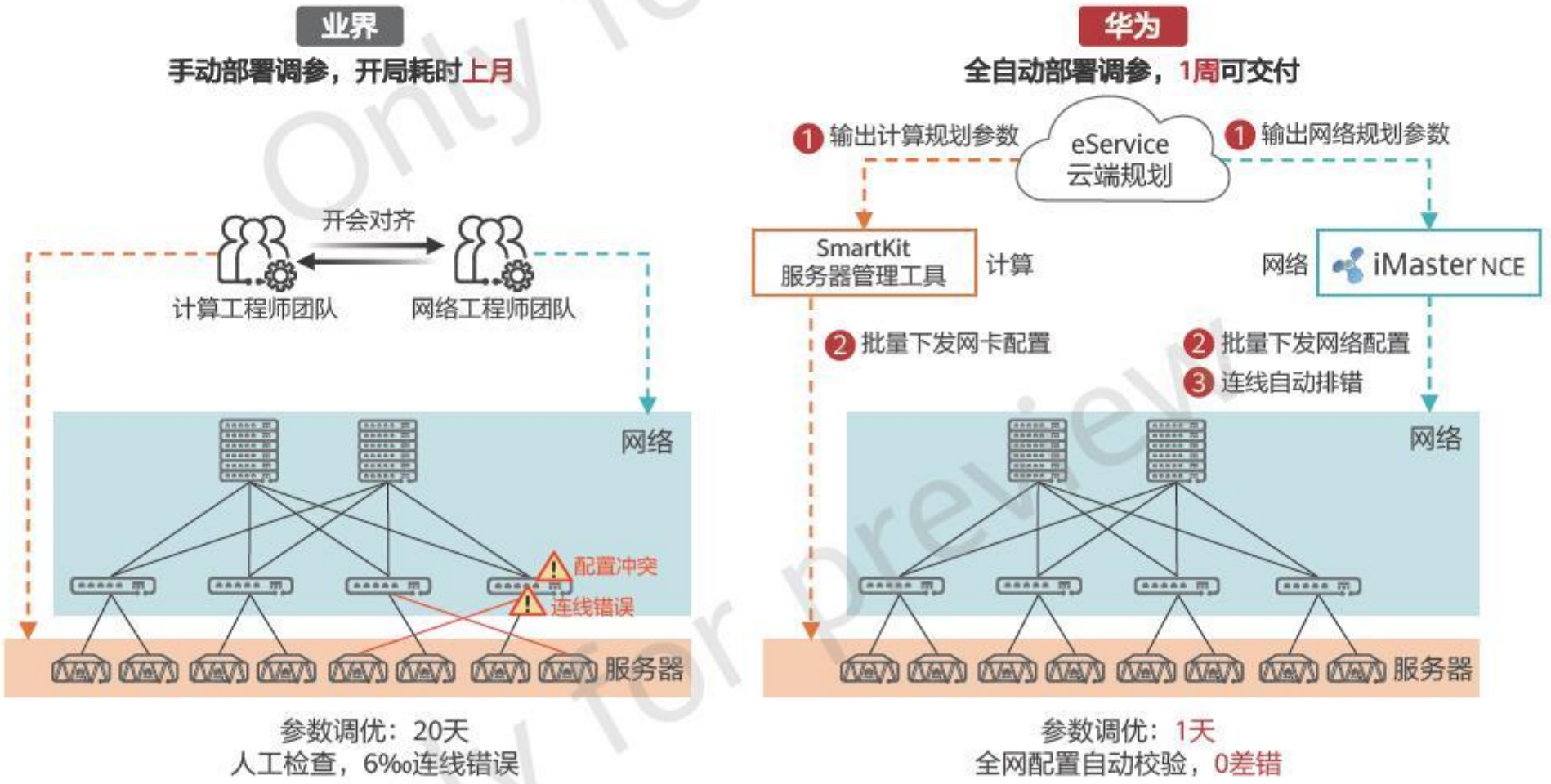


图2-4 传统部署方案与华为计算网络一体部署方案对比

» **价值4-网络关键指标全程实时可视，分钟级识别异常，排障效率提升90%**

AI训练任务一旦出现异常，快速排障恢复训练直接影响算力可用率。因此金融智算网络支持训前、训中的智能检查与定位须作为金融智算网络的建网标准之一。

华为基于计算、网络、存储一体化的iMaster CCAE（集群自智引擎）运维平台，在训练前可实施65项全量自检，保障网络100%健康。在训练过程中可实现跨计算、网络、存储的常见故障分钟级智能定界定位，覆盖300+故障模式库，整体运维效率提升90%。

某项目近2万个光模块，每年平均出现80+个光模块故障，每次手工排查耗时1天。华为可通过全面分析光链路多维指标数据，自动感知光链路亚健康，并结合华为独家AI预测算法，自动识别光链路脏污、松动故障，1分钟定位即可定位具体光链路异常，大幅提升运维效率。

2.1.4 成功案例：星河AI金融智算网络助力某客户大模型训练性能提升16%~23%

某客户数字化战略持续深化，在大模型研究和建设领域处于领先地位。当前训练的大模型，已经开始应用于客服、营销、运营等多场景。该客户现有数据中心智算网络遇到的业务痛点有：

- 交换机仍使用低密的400G线卡，无法做到100%线速转发。框框组网时，只能容纳2K~4K服务器规模，无法满足大模型训练需求。
- 交换机采用的是包交换，非信元交换，可靠性较差。
- 由于大模型训练流数少、单流带宽大、同步要求高，网络负载不均导致有效吞吐低至20%~50%。

使用华为星河AI智算网络解决方案后，给该客户带来如下价值：

- 华为提供36端口高密400G线卡，并实现100%线速转发，智算网络的组网规模是之前网络的16倍。
- 华为智算网络交换机采用信元交换，无阻塞转发，整机100%高速转发，时延抖动小，可靠性高。
- 华为独家的全网负载均衡技术，提升整网吞吐至95%，基于Bloom大模型性能提升16%，基于VGG16大模型性能提升23%。

2.2 AI赋能网络，打造智慧金融基础设施

金融行业正在从数字化向智能化演进，驱动金融业务持续创新。金融网络如何保障生产、保障运维和保障安全是金融客户普遍关心的问题。AI时代以智赋网，华为星河AI金融网络解决方案通过AI技术全面升级金融网络的运营、安全和节能能力，打造一个智慧、安全和绿色的全新金融网络体系，助力金融行业加速迈向智能化时代。下面描述的特性展示了AI在华为网络方案中的部分应用。

2.2.1 黑科技1：NetMaster网络大模型，让运维更智能

在网络大模型和运维体验方面，引入了700亿参数的网络AI大模型NetMaster，通过新的网络智能助手实现交互式的运营问答，大幅降低运维人员的技术门槛同时提升运营决策效率，比如无线园区用户投诉处置，通过快速的问答界面就可以在10分钟内解决无线接入认证等问题，处置时间缩短88%，员工投诉减少50%。

在园区网络和数据中心网络中，通过引入网络数字地图采集网络、流量、设备、服务器、应用等信息还原全网拓扑，可以实时呈现网络状态和业务路径，精准自动识别网络故障，实现隐患的深入分析与预防，让网络故障率降低90%。同时，通过业务仿真校验功能，预先评估实施方案的风险，确保网络配置变更100%正确。

2.2.2 黑科技2：智能未知威胁检测，让数据更安全

在网络安全方面，华为首创基于AI的智能未知威胁检测技术：首先通过自研MDL可编程病毒检测语言实现使用少量资源精准覆盖海量变种；同时，病毒扫描引擎也集成了针对未知威胁的多种专用启发式及神经网络智能检测算法，可精确防护亿级海量病毒。配合华为AI防火墙，可实现：

- 应用识别准：实现5大类57子类6000+应用识别，策略可控，流量可视。
- 入侵防御强：通过云端智能化签名生产，提高30倍生产效率。本地基线学习+黑样本增量学习，IPS阻断率是业界3倍。
- 恶意文件检出率高：CDE引擎支持百层级混合压缩和多层隐藏病毒检测，恶意文件检出率97%。

2.2.3 黑科技3：Wi-Fi 7动态变焦天线AI智能漫游，让体验更流畅

在园区网络无线场景，华为Wi-Fi 7产品推出了动态智能变焦天线、AI漫游等特性，有效解决人员动态聚拢和随机移动的体验问题。

动态变焦智能天线内置高密和全向两种模式，可根据用户密度动态调节天线覆盖范围。当覆盖范围内用户增多，AP自动切换成高密模式，如同加上虚拟灯罩，使信号更加聚焦，性能提升20%；而随着用户分散，AP则自动切换成全向覆盖模式，如同去掉了虚拟灯罩，信号覆盖面积也随之增大。

AI漫游技术在智能漫游的基础上，通过提高漫游灵敏度，实现终端移动漫游过程中的链路质量提升，让终端在漫游过程中也能保持好的信号状态。同时，通过AI算法采集终端漫游阈值、引导策略等信息并最终学习生成个性化的、自动更新的终端画像，通过该画像可以帮助终端提前识别更佳的漫游AP，漫游成功率从50%提高至98.5%，极大提高无线漫游体验。

2.2.4 黑科技4：AI算法与架构双创新，让投资更绿色

网络节能方面，针对办公室场所夜间网络无人使用的场景，华为基于园区数字地图直观呈现“全网-站点-设备”能耗，通过AI算法进行潮汐预测，自动推荐AP节能时段，典型场景可降低30%能耗，提高能耗利用效率。

另外，在架构侧，传统的组网是烟囱式建网，设备多，功耗大；华为的多网合一方案，通过一套物理组网承载多个业务网络，在逻辑上实现业务隔离，减少建网设备，功耗降低可达35%。

最后，华为Wi-Fi 7 AP在设备侧也通过无缆智能天线的极简架构，由传统的5层变3层，可使单设备功耗降低19%。

03 超高韧性，助力金融容灾无忧，业务永续

3.1 金融安全规范对数据中心网络的可靠性提出更高的要求

银监会在《商业银行数据中心监管指引》发文中定义6级灾难恢复能力，商业银行重要信息系统灾难恢复能力应达到《信息安全技术信息系统灾难恢复规范》中定义的灾难恢复等级第5级（含）以上，RPO为0，RTO为数分钟。金融对数据中心可靠性要求99.995%，全年业务中断时间26.28分钟，领先银行甚至提出5个9要求。

表 C.1 RTO/RPO与灾难恢复能力等级的关系

灾难恢复能力等级	RTO	RPO
1	2天以上	1天至7天
2	24小时以上	1天至7天
3	12小时以上	数小时至1天
4	数小时至2天	数小时至1天
5	数分钟至2天	0至30分钟
6	数分钟	0

图3-1《信息安全技术信息系统灾难恢复规范》定义的RTO/RPO与灾难恢复能力等级的关系（GB/T 20988—2007）

3.2 传统金融网络存在容灾能力弱、可靠性可用性不足等问题

基于安全规范和业务对网络的可靠性的要求，主备数据中心无法满足业务增长和高可用需求，逐步向多地多活数据中心发展演进。最低要求是核心系统主备，渠道、支付类业务多中心多活，网络多级保护、故障迅速感知定位，业务中断时间趋于0。因此目标网络韧性面临三大挑战。

» **挑战1-多DC容灾网络，跨DC灾备切换、设备和链路级故障，业务中断时间无法达到5个9容灾高可靠要求**

跨云跨DC部署分段打通，上线耗时数周，异构网络各自管控，复杂业务多断点，灾备场景RPO无法达到分钟级的标准。设备整机故障时，已有的主备保护方案无法做到无损升级。服务器接入侧链路故障收敛时间也在秒级以上。

传统的链路故障感知通常依赖BFD检测技术，对上下游设备互联端口进行定期故障检测，耗时在毫秒（ms）级别；转发面感知到故障后，通知控制面重新算路，全网路由收敛，生成新表项下发指导新的路径进行转发，整体耗时近1秒。

» **挑战2-金融网络大量的配置变更，完全依赖专家经验进行评估，无法避免部署错误，变更影响性更难以预测**

当网络变更需求发生时（例如：Underlay或Overlay网络变更，增删改配置，包括路由、逻辑网络、ACL等），通常都会组织网络专家团队评审，但大量历史配置仅依赖专家经验进行变更评估难免有疏漏，现网运维中仍然会出现大量的配置部署新问题，尤其是变更后的影响性、业务的连通性变化更难于预测。

» **挑战3-原FC网络扩容成本高，而传统以太技术易丢包无法支撑存储长距传输**

传统存储网络使用FC，而FC网络当前带宽普遍在16/32G，在同城双中心的传输上，如果是客户需要做一个400GE的互联，那就需要十条甚至几十条这样的FC链路，大幅增加整个链路成本。

采用以太的技术，虽然可以做到100G以及400G的互联，但长距的以太传输会因丢包导致整个时延的增加，进一步引起数据中心网络内反压的滞后性。两个常见的相距70公里的同城数据中心，网络的传输时间都会大于1毫秒左右，1毫秒会导致整个数据中心内部的存储反压机制的彻底失效。

» **挑战4-网络亚健康风险未知：故障被动投诉，网络质量无法提前感知。**

现网存在亚健康时，无法提前感知风险，只能被动响应随时可能发生的故障。缺少系统性的数据分析和评估，并对未来状态进行预判，难以系统性的掌控网络质量、全局评估网络风险。

3.3 星河AI金融数据中心网络方案，极大提升网络容灾能力和可靠可用性

为了应对这些挑战，华为发布了星河AI金融数据中心网络方案，使用独家全场景iReliable技术和潜在风险AI评估能力，极大提升了业务容灾能力和网络可靠性。

» **价值1-华为发布独家全场景iReliable技术，网络故障业务无感，应用故障快速切换。**

网络级高可靠：领先的仿真校验算法实现网络配置变更事前仿真，事后校验，配置100%准确。多DC提供网络级主备/双活出口容灾，实现业务自动切换。主备DC间快速切换，网络升级零丢包。

设备级高可靠：M-LAG无损升级，支持通过SDN控制器实现智能引流，整个升级过程业务0丢包。

链路级高可靠：华为独家DPFR技术，实现故障快速感知，设备互联链路亚毫秒级切换。通过硬件感知上下游互联链路，DPFR数据面感知到故障后，根据预制规则切换链路。故障感知从控制面变更成转发面，故障切换时间从100ms缩短到1ms。

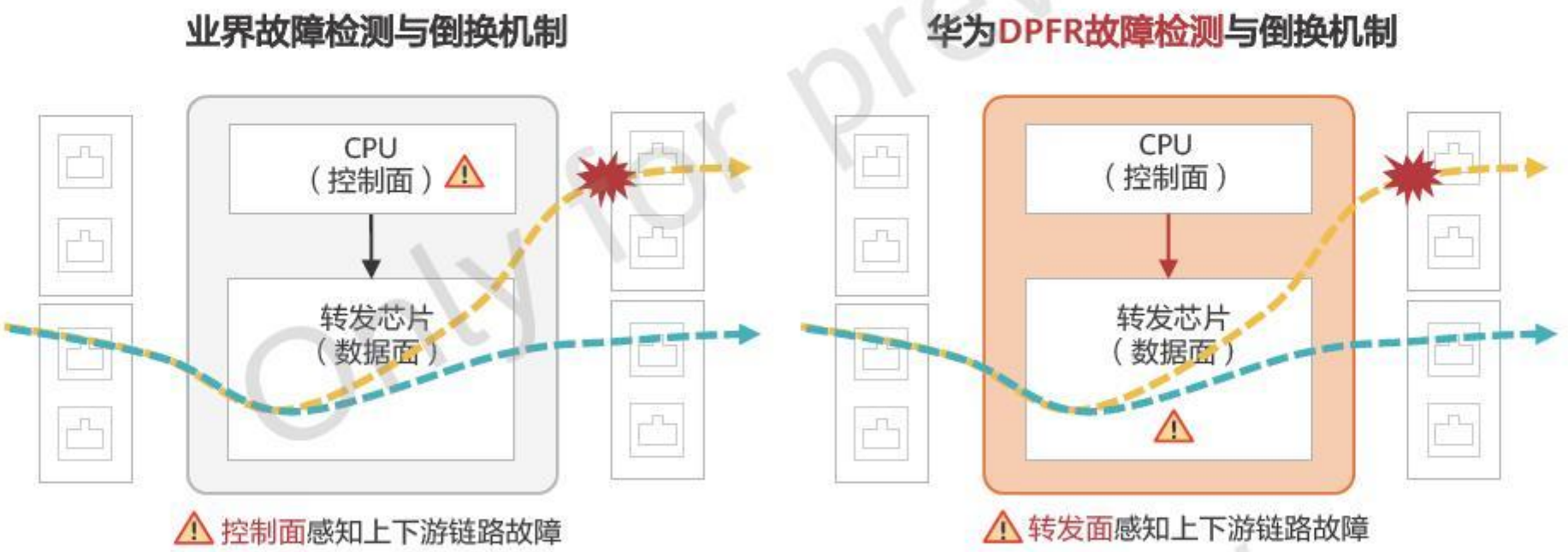


图3-2 华为独家DPFR技术

» **价值2-华为iMaster NCE-Fabric仿真技术实时呈现网络变更影响，提前发现100%配置问题**

华为iMaster NCE-Fabric会实时收集当前数据中心网络拓扑、配置、逻辑资源等数据信息，根据采集到的现网信息进行Underlay、Overlay网络建模，基于报文头空间算法进行建模，将网络模型转换成转发函数，进行意图的数学求解；最后给用户提供以下业务价值：

资源占用评估：网络变更导致的VRF、Static Route、L2子接口、VNI、BD、EVPN等逻辑资源占用情况变化，有效避免资源超限引起的配置失败问题，并提前提示用户做网络扩容。

全网影响性分析：通过仿真识别网络变更前后全网IP连通性变化，便于用户做判断和处理。

连通性分析：基于特定IP五元组会话的连通性变化仿真结果，将存在影响的异常情况以路径方式直观的呈现，使用户更精确的预判连通性问题点。

» **价值3-华为ilossless智能无损方案支持100KM长距无损，同城双活跨DC链路减少90%，数据0泄露**

华为全方位升级iLossless智能无损方案，在原基础上引入了时间、空间维度和流量预测算法。能够在设备的原端提前感知流量，预测下一时刻的流量变化范围，从而在整个数据源端预判业务拥塞情况，并做流量的提前控制。华为支持100公里2*100G大带宽情况下，同城传输智能无损，大幅节约了跨城传输的链路。同时，CloudEngine系列交换机支持MACsec加密，保障跨DC数据输出的0泄露。

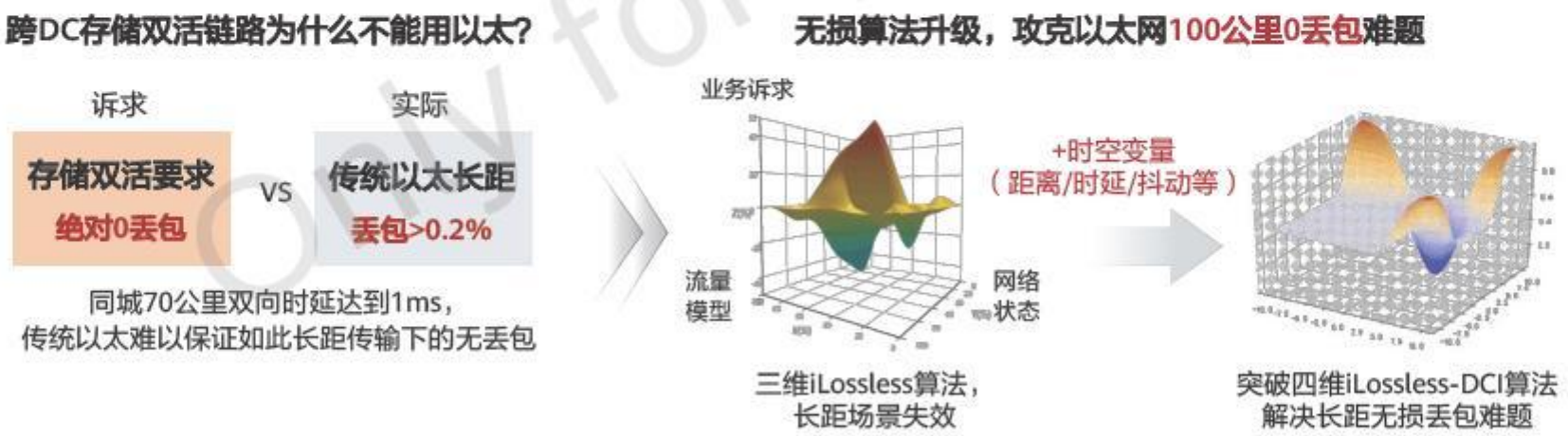


图3-3 华为全方位升级iLossless算法，攻克以太网100公里0丢包难题

» **价值4－网络风险主动评估，故障提前规避**

硬件亚健康主动检测，业务受损前识别风险：某客户网络中光模块长时间运行，光器件性能衰减，导致链路不稳定。光模块问题现象无规律，难于复现，且定位周期长，业务稳定风险非常高。通过关键KPI指标数据基于Telemetry主动上报，海量数据分析，创新相关性检测算法，提前识别亚健康光模块/光链路（仅支持华为认证光模块），运维人员可提前介入更换器件，从而避免故障发生。

网络级风险及时发现，快速闭环恢复：某客户Fabric网络中可能存在VXLAN的下游网络出现环路，管理员需及时发现环路问题，并识别出环路的设备和端口，环路问题影响大，急需及时恢复业务。通过基于Telemetry+Syslog机制监控所有接口的KPI及异常日志，识别疑似二层环路接口，做到快速定位故障，并呈现环路接口列表及位置，联动控制器隔离环路接口，提前规避潜在风险。

3.4 成功案例：华为助力Z银行构筑敏捷弹性、高可用的新一代云数据中心网络

2017年以来，Z银行已形成较为完整的三中心布局，有效支撑了业务的快速发展。由于已有云平台在扩展性、可靠性、性能、运维自动化程度、网络服务软件化以及服务化能力等方面存在不足，对生产运维管理带来以下挑战：

- 网络运维效率不高：新云架构软网元的运营和运维手段不足；传统网络、硬SDN和软件SDN等异构网络并存，缺乏多点协同能力。
- 网络可用性架构不完善：配置变更风险大，存在高危命令操作，无配置前校验和仿真验证的有效手段。网络无告警的“亚健康”网络假死问题（如光模块失效、CRC异常、端口/单板假死等）存在重大事故的隐患故障恢复时间长，极端情况下全面恢复超过3小时。
- 网络性能容量不足：融合数据湖数量分析量急速增加，大数据分析、分布式存储、AI训练场景网络带宽不足，易出现网络拥塞。

华为联合该银行构筑新一代云数据中心网络，不仅满足业务发展对网络灵活多变的诉求，极大提升了云管平台的可用性和新云网络与现有网络的互联互通性能。

- 敏捷弹性：软件SDN与底层硬件解耦，解除厂商绑定，SDN技术快速迭代，满足业务发展对网络灵活多变的诉求。基于NFV软件网元提供网络服务，实现网络服务的灵活弹性、敏捷供给、与硬件解耦。SDN + NFV在金融数据中心生产环境大规模使用，业界首创，开金融行业ICT技术之先河。
- 高可用性：集群方式部署NFV网元；双AZ方式部署业务；云管平台跨Region主备方式部署，提升总体可用性；部署iLossless智能无损方案，同城传输智能无损，大幅节约了跨城传输的链路，并解决网络反压延迟问题。
- 极致性能容量：10G接入+40G互联，优化为10G接入+100G互联；DCI同城互联扩容到1T，极大改进了网络的转发性能容量，支持业务未来5~8年的发展。高性能硬件专线网关出口，极大提高了新云网络与现有网络的互联互通性能带宽。
- 高可靠性：Underlay网络做M-LAG、BFD、分层分布，极大增强了网络级和设备级可靠性；部署DPFR技术使连路级故障恢复时间缩短到1ms。

04 敏捷高效，实现网络自动驾驶

4.1 网络数字地图助力金融产品敏捷开发，提升金融业务上线效率

4.1.1 金融业务的快速迭代，对网络运营提出了更高要求

金融业务的数字化带来了海量的应用创新，新业务上线速度和网络运维管理提出了更高的要求。国内大行每年有上万次新版本新应用上线，绝大部分业务上线或升级都涉及网络变更，因网络变更对业务的影响评估不准导致生产业务中断时有发生。如何实现网络全面、敏捷、智能的管理和运维成为关键挑战。

4.1.2 越来越频繁的网络变更，网络运维判不准、看不全、看不清、耗时长

» **挑战1-判不准：每年上万次新版本上线，人工评估网络变更风险耗时耗力，无法支撑业务迭代效率**

某银行全年网络变更14000+次，曾在网络变更时，因为变更考虑不周引发BGP路由冲突，而网络故障普遍具有实时性，因此导致业务中断。

» **挑战2-看不全：云化改造导致无法实时动态感知现网变化，传统运维模式无法实时联动业务状态**

某银行随着业务全面云化改造，计算和网络均采用虚拟化技术，网络就像黑盒，运维人员仅能看到拓扑、设备状态、端口流量等信息，即使感知到某设备的某端口拥塞，但是无法精细获知哪些业务会受影响。为了建立网络运维全景基线数据，该银行投入10+人力梳理了三个月，但是全网拓扑准确度仍然不足60%，也无法实时动态感知现网变化。

» **挑战3-看不清：超大规模的业务和网络模型，20+运维系统相互割裂，导致业务故障无法快速定位**

某银行有20+资源池分区、1万+网元和3300+应用，20+运维系统相互割裂。为了避免对银行业务造成影响，运维人员需要及时处理单点网络报障，然而实际情况中出现业务故障后，负责不同系统的运

维人员因为缺少协同手段，大多串行进行故障隔离，平均排障时间达到数小时或者数天以上。

» **挑战4-耗时长：安全策略与网络连接相互耦合，配置变更耗时长，大量历史冗余配置加大了运维难度，防火墙10万条安全策略验证耗时2人月**

在银行网络的日常变更中，防火墙变更耗时占整体运维耗时超50%，分析工单的流量路径、防火墙生效位置、策略和配置的人工生成和下发等消耗大量人力和时间。例如某银行防火墙10万条安全策略验证耗时2人月。

另外，由于火墙配置冗余严重，单台防火墙设备策略查询时间为小时级，已有部署策略无法评估是否冗余，大量容冗配置难以删除。

4.1.3 华为率先在业界推出网络数字地图，推进金融网络运维智能化

华为一直在思考，如何帮助客户有效解决上述难题，经过数年与国内头部客户在网络运维数字化领域的创新实践，华为率先在业界推出网络数字地图。网络数字地图就像日常生活中频繁使用的地图类APP，除了具备实时路况导航功能外，我们还可以在地图APP上打车、搜餐馆、订酒店，它已经成为我们数字生活不可分割的重要部分。

能力维度1	Level 1基础监控	Level 2进阶监控	Level 3性能监控	Level 4业务监控
网络监控（40%）	事件监控 基础监控：Trap告警、Syslog监控 基础告警：网络设备状态、接口、单板、CPU告警	指标监控 进阶监控：集成网络、系统、应用监控、融入运营流程 进阶告警：时间关联分析、性能趋势分析、SLA 报表审计	性能监控 精细化监控：包检测、流分析、协议性能分析 基于ITOA深度运营 故障自愈：主动识别+自动化处理	业务协同监控 应用与网络协同监控 故障自愈：数据模型驱动的未知故障发现和故障学习 智能学件发布
能力维度2	**Level 1文档化**	**Level 2信息化**	**Level 3数字化**	**Level 4孪生化**
网络管理（30%）	基于文档/表格 人工申请资源 手绘网络拓扑 数据文本化管理	基于CMDB 标准化资源申请 静态资源管理 静态网络拓扑 数据半结构化管理	基于网络数据中台 定制化资源申请 动态资源管理 网络数字化建模（SSOT） 动态网络拓扑 数据模型化、结构化管理	基于数字孪生 智能资源分配 资源趋势分析 应用/ 网络拓扑 数据图谱化管理
能力维度3	**Level 1工具化**	**Level 2平台化**	**Level 3服务化**	**Level 4智能化**
网络控制（30%）	基于CLI工具 脚本生成工具 设备批量配置工具 表更批量检查 设备巡检工具	基于场景自动化平台 数据产生和消费的数据架构 整合工具统一界面 配置校验 网络功能虚拟化	基于服务化控制中台 iBPM网络服务灵活组装编，快速发布 微服务架构 面向服务的API接口 网络仿真 网络DevOps	基于智能学件、算法驱动的智能自动化平台 基于数据驱动实现决策自动化 跨域、跨界的场景整合 机器人硬装作业

图4-1 金融网络数字化转型评级标准（出自：《金融数据中心网络数字化能力建设研究报告》，北京金融科技产业联盟，2023.7）

华为 iMaster NCE 网络数字地图就是把物理网络中数百万级的链路映射到逻辑世界，让整个网络（包括设备、链路、连接、应用、用户等）能被看得见、看得清，这相当于给金融网络装上一副透视眼镜，可以洞悉一切，从而打造一个网络世界的数字空间。华为 iMaster NCE 网络数字地图在金融网络数字化转型评级标准中的网络监控、网络管理和网络控制三个层面已处于 Level 3~Level 4 的领先水平，华为 iMaster NCE 网络数字地图有以下三大核心价值。

» **价值1-网络变更1秒仿真，变更0出错，支撑金融业务快速上线**

华为发布业界首创的网络数字地图技术，在金融业务上线场景中，跨云跨分区异构网络变更可视，通过“仿真+验证”的方式，节省了专家评审和反复修改配置方案的时间，使网络变更100%获得部署前的影响分析和仿真验证，支撑金融业务快速上线。

» **价值2-多云网络1图呈现，准确率高达99%以上，支撑金融业务实时感知**

华为网络数字地图通过Telemetry技术、IPCA（Packet Conservation Algorithm for Internet，网络包守恒算法）技术全方位感知网络状态、终端连接状态、应用状态，并通过AI智能拓扑还原技术，使金融企业网络全貌、数据中心内网络和单区域内网络这三个层级的拓扑逐级精细化可视，多云网络拓扑精准识别和还原。运维人员可以清晰地看到业务与网络状态并主动维护，准确率高达99%以上。

» **价值3-网络故障3分钟定位，支撑金融业务异常分钟级定界定位**

华为基于30多年的网络运维经验，总结了大量网络故障库，并通过知识图谱等算法实现故障推理和分钟级根因定位。例如当故障发生时，可以看到应用流量经过的真实网络路径以及每个网络节点的丢包和时延等指标。如果流量异常，会自动在拓扑上呈现并给出异常分析结果和处理建议。同时，通过40+关键网络风险预测项，构筑主动预防体系，将“救火”变为“防火”。

» **价值4-自动化管理防火墙海量策略，工单处理时间缩短到1分钟以内**

华为推出防火墙策略全生命周期管理方案，通过网络拓扑和安全矩阵仿真技术，实现新开通业务的策略路径自动还原、策略路径可视，防火墙策略自动化管理及配置自动下发，降低人员手工配置工作量，减少人为错误，提升防火墙运维效率。

该方案还可主动收集现网防火墙策略信息，结合系统的安全策略大纲，分析防火墙策略的命中和冗余情况，智能识别异常策略和冗余策略，定期清理冗余策略。该方案同时支持异构厂商的配置管理。

4.1.4 成功案例：华为网络数字地图助力X银行网络拓扑准确率99%，业务上线时间从周缩短到天

华为数据中心网络全球交付超两万家客户，网络数字地图作为业界首创，已在多家银行成功落地实践。某银行基于华为网络数字地图打造的智能导航系统，拓扑准确率99%，业务上线时间从周缩短到天。

该银行是全国12家股份制商业银行之一，为了打造并快速推出新产品，采用敏捷开发方法快速响应业务部门的需求变化，打造实用有效的100+项创新应用，彰显有辨识度、有影响力的金融科技成果。

该银行现有网络运维系统20+个，2.5万个虚拟机上承载的应用每天都有新需求，每年上万个新应用版

本的上线对网络运维团队提出了巨大挑战。首先，业务上线流程非常严谨，复杂的网络配置变更需要经过数周时间梳理，数周专家评审，但即使这样，每次业务上线，网络部门还是像走钢丝一样提心吊胆。其次，2023 年上半年真正由网络引起的生产问题仅占 4%，其余 96% 的问题都出在应用和数据库上，网络部门无法快速自证清白，持续协同其他团队定位导致运维工作量增长近 20 倍。如何既能满足业务敏捷迭代开发对网络变更的诉求，又能在业务异常时快速定界网络故障成为该银行的痛点。

该银行基于华为 iMaster NCE 网络数字地图打造的数据中心智能导航运维系统，能够全局感知 2000+ 设备、2.5 万个虚拟机的网络运行情况，拓扑准确率达 99%，业务按天级时间上线。首先，通过事前仿真校验，杜绝人为差错，保障了网络配置变更 100% 准确，节省了专家评审和反复修改配置方案的时间，实现了业务快速、安心上线。其次，独家的应用网络一体化运维，使应用与网络协同定位效率提升 90%，做到了分钟级故障定界定位。

图4-2 某银行数据中心智能导航定位系统

4.2 金融广域网络“IPv6+”全面部署，保障金融客户多地多中心灵活高效互联

4.2.1 金融业务数字化高速发展，对广域网络服务质量提出了更高要求

国家战略层面强调要深入推进金融行业IPv6规模部署和应用。八部门联合印发《推进IPv6技术演进和应用创新发展的实施意见》：到2025年底自主创建50个以上“‘IPv6+’创新之城”，每个重点行业打造20个以上应用标杆；打造超过1000个支持“IPv6+”技术能力的承载网络、企业/园区网络和数据中心；新开通的IP专线业务，50%以上采用SRv6等创新技术。

（三）主要目标

到2025年底，IPv6技术演进和应用创新取得显著成效，网络技术创新能力明显增强，“IPv6+”等创新技术应用范围进一步扩大，重点行业“IPv6+”融合应用水平大幅提升。

——技术创新取得显著突破。在基于IPv6和“IPv6+ ”的新型网络体系、算力网络、确定性网络、网络内生安全和绿色节能等创新领域取得显著突破，部分重点方向的技术能力国际领先，IPv6演进技术标准体系基本形成，国际标准化贡献率进一步提升。

——产业支撑能力大幅提升。初步形成以IPv6演进技术为核心的产业生态体系，网络芯片、模组器件、整机设备、安全系统、专用软件等研发能力持续增强，分段路由（SRv6）、网络切片、随流检测、应用感知网络（APN）和网络智能化等成熟的“IPv6+”技术实现产品化落地，在基础网络、行业网络、园区网络、数据中心等场景中得到规模化应用，建成一批创新公共服务平台，有力支撑技术创新、系统试验和产业推广。

——基础设施能力持续增强。骨干网、城域网、5G等基础网络基于IPv6进一步升级演进；在企业组网和上云等场景中，新增用户开通的IP专线业务50%以上采用分段路由等创新技术；新增网络基础设施和应用基础设施规模部署IPv6单栈；不再新增部署面向互联网用户的IPv4到IPv4网络地址转换（NAT）设备，加快存量设备退网；打造超过1000个支持“IPv6+”技术能力的承载网络、企业/园区网络和数据中心。

——重点行业应用成效凸显。政务、金融、能源、交通、教育、制造等行业和领域，在IPv6规模部署基础上实现“IPv6+”技术的广泛应用，每个重点行业形成20个以上应用标杆。支持各IPv6技术创新和融合应用综合试点城市先行先试，加快推动IPv6技术演进发展，自主创建50个以上“‘IPv6+’创新之城”。

——安全保障能力显著提升。建成高效可靠的IPv6网络安全技术手段，IPv6安全技术创新能力大幅提升，IPv6网络安全产品和服务广泛应用，IPv6网络安全防护与检测监测体系不断优化完善。

图4-3《关于推进IPv6技术演进和应用创新发展的实施意见》中的主要目标

4.2.2 传统金融广域网面临着扩容成本高和部署慢的问题

» **挑战1-成本高：金融业务增长带动专线带宽持续扩容，费用持续增长，且链路利用不均衡**

业务的快速增长带动海量数据在银行多个数据中心、分支行、办公机构间高速交互，经常导致多条链路负载不均衡，需要扩容线路带宽。某银行为了应对带宽持续增长、链路利用不均衡的问题，专线带宽每年扩容30%，导致带宽租赁费用每年高达20亿，租赁费用是设备采购费用的4倍，给客户带来巨大成本压力。

» **挑战2-部署慢：金融业务多地多活部署，大量数据中心间的网络开通需要人工部署，费时费力**

面对业务跨数据中心互访、多活负载的诉求，多数据中心的网络需要能够根据业务变化快速自动编排。某银行原有的同城数据中心其物理容量和扩展能力已无法适应大规模和高灵活性的业务接入需求，该银行在原有两地三中心的基础上，规划陆续多个异地新数据中心，计划在2025年完成三地六中心的多活架构。大量业务的跨数据中心部署以及按需互联互通的需求爆发，对跨数据中心网络的规划、配置和运维都带来极大挑战。

» **挑战3-定位难：金融业务流量路径未知，业务受损时无法迅速定界和定位故障节点**

国内大行/股份制银行运维部门反馈，随着骨干网络规模越来越大，故障定界定位时间变长，以往多依赖人工经验分析的维护方式已无法满足故障快速定位诉求。银行骨干网SRv6隧道采用单CP多SList方式，路径自动分裂，流量自动调优，运维人员无法感知具体业务路径，故障发生后定位难。

» **挑战4-感受差：网络高峰时段，广域网络易拥塞，导致关键核心业务受损**

某银行在现有网络高峰时段，广域网络拥塞情况下，生产等关键业务与备份等非关键业务同级别调度、同路径转发，导致关键核心业务受损。另外，未能按VPN颗粒度充分调度，导致线路利用率不均，线路租赁费用无法有效下降。

4.2.3 华为“IPv6+”智能云网方案实现多地多活云网协同、智能调优和差异化服务

面对金融客户多地多中心间网络协同难、链路利用不均衡的挑战，华为提供“IPv6+”智能云网解决方案。方案涵盖了网络协议简化、SRv6路径可编程提高专线利用率、数据消冗降低带宽需求、iFIT随流检测快速定界定位、APN6提供差异化SLA、自动化编排发放网络配置实现业务灵活部署等优势能力，满足金融客户多地多中心灵活高效互联的诉求。

» **价值1-广域网络智能调优提升链路利用率20%，网络数据消冗节约45%的带宽资源，极大节省了专线租赁费用**

基于华为NetEngine系列路由器的SRv6技术和iMaster NCE的SDN能力，实现金融广域网络流量智能调优，**提升链路利用率20%**，保护线路投资。某银行链路调优后广域链路资源利用率**提升20%以上**，关键业务**时延最大降低46%**。

在金融骨干网按需部署网络级数据消冗，可有效缩减骨干网数据传输量，节省带宽资源和专线租赁费用。某银行骨干网2023年采用华为网络级数据消冗方案，将数据中心间的DB异步复制、磁盘异地复制等灾备流量从原来的**10.8Gbit/s压缩到5.8Gbit/s，节约45%的带宽资源**，极大节省了专线租赁费用。

» **价值2-iFIT随流检测技术实现业务状态实时监控、业务路径可感知、网络故障快速定界定位**

通过端网同时部署iFIT，端到端检查应用网络状态，检测网络抖动、丢包率等指标。iFIT还可实现逐跳网络KPI测量、业务丢包溯源、物理路径还原呈现，如有异常可实现快速定界定位。同时，基于真实业务流染色，而非拨测技术，检测结果更加准确。某银行在分行到数据中心间部署iFIT来监测关键业务，实现了分行到总行间线路的可视化故障监测和定位。

» **价值3-APN6技术实现应用自驱动选择网络服务，确定服务级别，确保差异化SLA和关键业务无损**

金融骨干网基于APN6入隧道提供差异化SLA。通过IPAM集成APN-ID资源管理功能，北向提供用户配置入口，南向推送应用的网络需求给网络控制器。同时主机端侧获取自身服务的APN-ID。现有应用无需改动，即可在主机内部完成APN6的标识，最终使业务流量根据不同的APN6标识进入不同隧道，实现业务的差异化LSA保障。

» **价值4-基于华为MDC方案，统一运维入口，分钟级自动下发跨数据中心的网络配置，支撑金融业务灵活部署**

华为MDC（Multi-DC）方案可实现跨数据中心的统一资源管控、网络业务的可视化编排和自动化发放，极大提升网络部署效率，加速了跨数据中心资源域互联互通建设。某银行通过华为MDC跨数据中心协同方案，实现分布式数据库、互联网接入资源池、生产云资源池等多个关键生产业务按需互通的统一编排，网络开通周期**缩短至分钟级**。华为MDC方案已作为该银行多数据中心互联的关键底座，支撑该银行向多地多活架构演进。

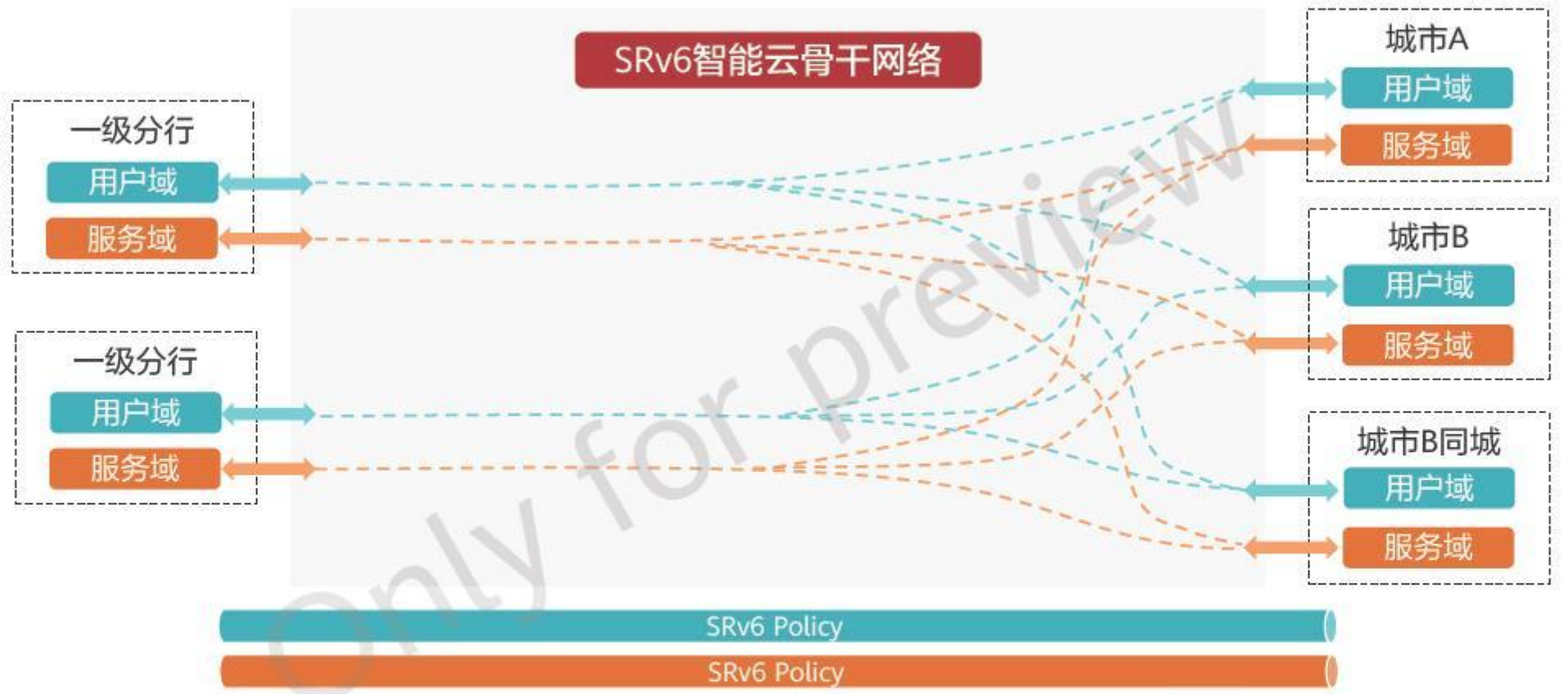
4.2.4 成功案例：华为SRv6智能调优方案，助力Y银行带宽利用率提升20%

金融行业全面推进IPv6技术创新与融合应用，华为“IPv6+”智能云网方案已在六大行、半数以上的股份制银行成功部署上线。

某银行为了支撑服务生态化战略，构建多中心业务架构，业务的互访关系变得更加复杂，骨干网数据流量快速增长。传统骨干网从潮汐式规律流量变成随机突发型流量，数据突发无法提前预测，因此该银行只能以峰值数据来租赁带宽。例如某一级分行平时流量带宽在300M左右，峰值带宽高达500M，导致多租用60%带宽。另外，专线拥塞后没有可行的调优手段，只能购买额外带宽，增加了成本。尤其是DC间异地灾备流量，已超过DCI总流量的50%，但这又属于“硬性支出”，没法降低。

面对这些问题，该银行骨干网络技术栈不断迭代升级，从MPLS到SR-MPLS，再到现在的“IPv6+”方案。该银行的整个骨干网通过部署华为SRv6智能调优方案，将该行三大数据中心以及近40个一级分行全面互联。另外，该银行基于IPv6的OASS内网应用，试点端侧部署APN6能力，骨干网基于APN6入隧道提供差异化SLA保障。同时，该银行已完成端到端iFIT的骨干网部署，实现业务丢包快速溯源，加速了网络故障的定界定位。

如下图所示，该银行在链路调优后资源利用率**提升20%以上**，关键业务**时延最大降低46%**，业务开通周期**缩短至分钟级**，每年专线费用**节省数千万元**。该银行网络负责人在采访中表示：“金融行业SRv6骨干网的架构和部署的模式业内已经形成共识，复制推广成功率很高。同时，受益于“IPv6+”技术强大可编程与调优能力，金融业务可以获得更好更快的业务体验。这些都能够为更多金融机构向“IPv6+”技术演进带来更加充足的信心。”



- 整网资源利用率提升20%
- 关键业务时延最大降低46%
- 业务开通周期缩短至分钟级
- 每年专线费用节省数千万元

图4-4 某银行SRv6智能云骨干网络方案

05 安全可信，保障金融业务安全

5.1 金融智能安全防勒索，多层防护构筑坚固堡垒

勒索软件（Ransomware）又称为勒索病毒，是一种恶意软件。勒索软件通过加密或锁定用户文件、屏幕、数据等计算机资源，导致数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。勒索软件危害的数据资产包括文档、邮件、数据库、源代码、图片、压缩文件等多种文件。受害者需要支付一定数量的赎金，才有可能重新取得数据控制权。勒索软件的赎金形式包括真实货币、比特币或其它虚拟货币。

5.1.1 勒索攻击愈发频繁，金融业务长时间中断风险激增

2023年全球勒索攻击率同比增长超37.75%，有效攻击载荷激增57.50%，支付赎金达11亿美元，平均勒索赎金达154万美元，同比增长100%，攻击平均导致24个工作日的系统停机。黑客利用网络钓鱼、暴力破解、零日漏洞等手段频频发起攻击，严重影响全球各产业数字化转型速度和效率。近年来金融业务因为勒索软件遭受巨大损失，例如某银行金融服务遭受勒索软件攻击导致部分系统中断，以至于不得不通过传统手动传递结算信息的方式来完成金融交易。

5.1.2 勒索病毒千变万化，传统网络安全面临新挑战

勒索软件已成为全球金融行业的主要网络威胁，面对勒索病毒的猖獗攻击，金融网络安全部门极其关注，对网络安全建设提出了更高的要求，金融行业需要精准的勒索病毒防护方案。当前主要存在三大挑战：

» **挑战1-病毒检出难：变种复杂繁多，年增长率近46%，普通静态签名匹配检出率低**

近年来随着勒索攻击专业化、团队化运作，勒索攻击手段日趋成熟、攻击目标越发明确，模式多种多样，攻击愈发隐蔽，病毒变种数量几乎呈指数上升，年增长率近46%。某银行进行网络安全防护测

试，发现有20%的新型勒索病毒能够逃避检测系统，现有防护系统面临较高的勒索风险。

» **挑战2-病毒扩散快：勒索病毒每分钟平均感染100万台终端，可完成2.5万个文件加密**

由于金融分支互联等业务需求快速发展，网络边界逐渐泛化，勒索软件一旦进入实质的攻击环节，其加密速度和窃取权限的速度非常快，勒索软件每分钟平均感染100万台终端，留给管理员处置的时间窗口期非常短。在一次勒索攻击中，某银行不到2小时就有20万个文件被锁死，现有的孤立处置方式很难阻止病毒的快速扩散。

» **挑战3-业务恢复难：传统全量数据备份慢，30TB数据平均需要1小时才能恢复**

最新的勒索软件攻击目标一般是银行备份系统、设备和虚拟机。传统备份形式的三件套是快照、备份存储、离线磁带库，快照容易被篡改，备份存储有被锁定的风险，离线磁带库性能过低。对被攻击的全球金融机构进行统计，发现超过46%交付赎金的银行也无法完全恢复数据，而能够恢复数据的银行，恢复速度最快也只有30TB/小时。

5.1.3 华为安全防勒索技术，构建基于完整攻击链的全网防护体系

华为基于勒索病毒攻击流程，提供业界唯一“端网存”多层防护方案：事前通过AI防火墙有效防御新型暴力破解，结合暴力破解行为特征，通过机器学习分类算法，避免密码被破解；事中利用独创内存溯源图谱算法快速溯源，HiSec Insight分析器通过网安联动和网存联动实现病毒隔离；事后独家网存联动实现系统数据快速恢复，如下图所示。

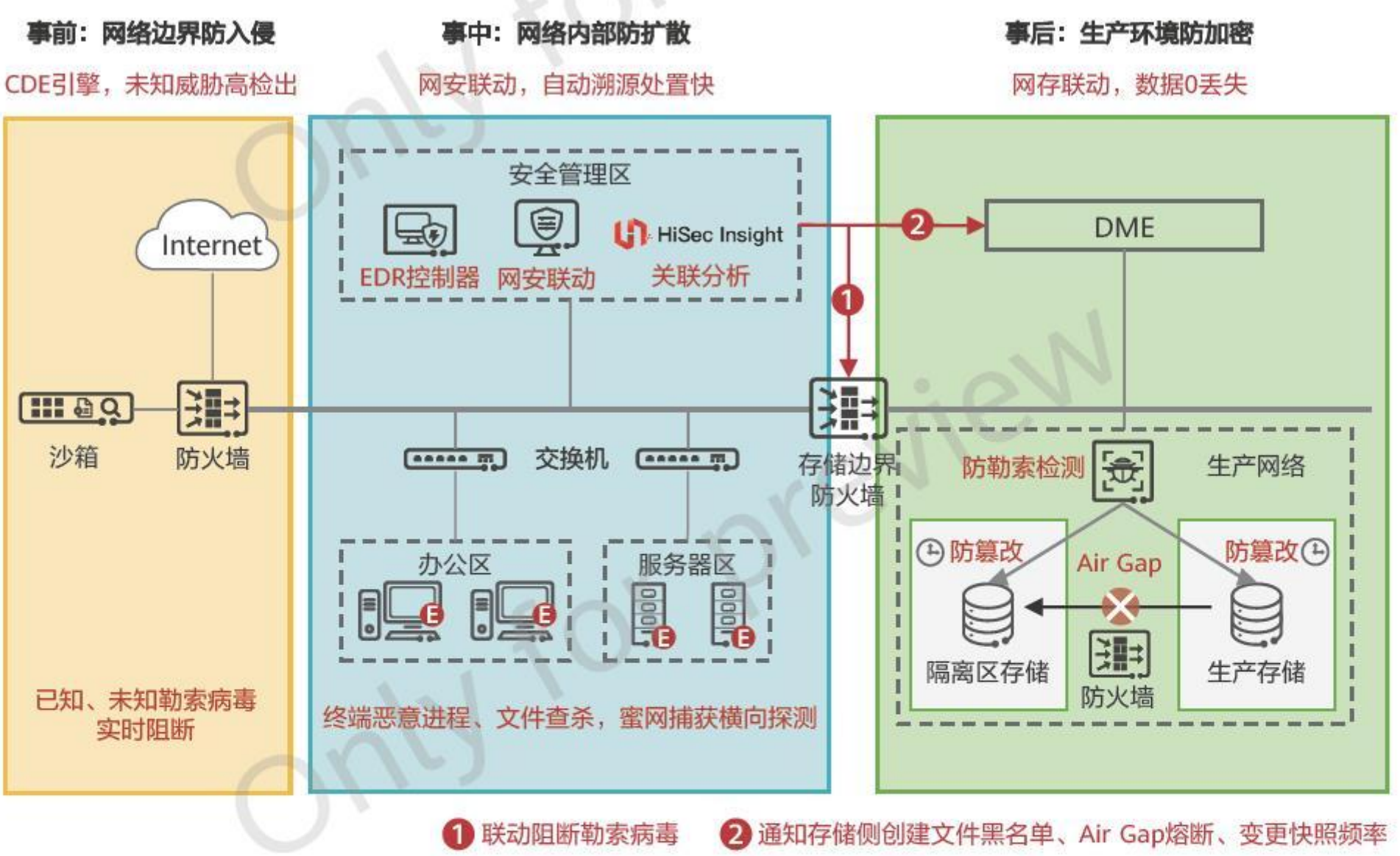


图5-1 华为“端网存”多层防护方案

事前、事中、事后对应三大价值如下：

» **价值1-威胁高检出：AI检测率90%以上，高出业界10%**

AI防火墙采用基于AI的检测引擎和算法，实现勒索病毒的智能分析，支持的病毒样本数量超过3亿，支持细粒度监控勒索病毒，文件类型维度的检测数量超过50，API维度的监控数量超过2000。某银行使用华为AI检测方式后，全面识别未知恶意软件，检测率从原先友商的的80%提升到90%以上。

» **价值2-溯源快处置：分钟级溯源处置，业界长达数小时**

安全态势感知系统收集现网的安全威胁信息，通过网安协同快速阻断威胁扩散，独家网存联动防止病毒横向扩散。业界人工取证、分析、溯源再配置策略的方式，单事件闭环时间至少需要2小时，某银行在引入华为解决方案后，实现了分钟级的安全分析和处置策略下发，有效阻止了病毒的扩散。

» **价值3-数据快恢复：数据恢复速度170TB/小时，比业界提升5倍以上**

网络态势感知系统可将勒索攻击告警实时同步给存储管理器，快速联动执行快照恢复、数据隔离、恶意文件黑名单等处置动作，避免病毒文件被备份。某银行引入华为独家网络和存储联动技术后，数据恢复速度高达170TB/小时，比业界提升5倍以上。

5.1.4 成功案例：华为构建领先的多层保障体系，打造安全运营环境

某银行拥有SOC安全运维团队，但是缺乏应对高级威胁的检测和分析工具，客户希望提供对APT高级威胁全面检测的手段，并能够跟踪APT的攻击路径、造成的危害和损失。

该行现网部署了上网安全桌面、友商防病毒软件，但仍存在风险，分行为安全短板，分行成为攻击总行的跳板。华为针对以上痛点，为客户构建防勒索病毒的安全保障体系：

- 在邮件服务器前部署FireHuner，用于分析外网发到本行的恶意邮件，从而发现基于邮件的渗透。
- 通过FireHunter + HiSec Insight分析总行内网到互联网的威胁，发现WEB渗透、C&C通信、外发数据等多种威胁。

该方案上线2个月后，效果明显：检测出8个新型勒索软件、9台被国内外黑客控制的服务器，以及34个现网防病毒软件没有告警的勒索病毒。

5.2 金融终端安全无感接入，防仿冒防私接

5.2.1 各类物联终端广泛应用，提升金融业务效率的同时，带来安全隐患

金融网点和园区在数字化、智能化转型升级过程中，通过引入各种物联终端，应用在客户服务、业务办理、数字化办公、智慧安防和能源管理等多个方面，提升了客户体验和服务质量，提高了运营效率。但同时大量物联终端的联网诉求，也增加了银行网络的风险暴露面。据《2024年上半年数据泄露风险态势报告》等权威报告显示，金融行业的数据泄露事件数量居高不下，其中不乏因终端仿冒接入网络、内部员工网

络私接等行为导致的泄露案例。

5.2.2 海量终端联网，对网络安全提出更大挑战

物联终端在金融网点和园区智能化转型中发挥着重要作用，但同时对金融网点以及园区的网络带来以下挑战：

» **挑战1–哑终端的安全性较低，网络安全威胁日益严峻**

在金融网点和园区网络中，接入设备数量急剧增加，同时网络攻击手段也变得更加复杂和隐蔽。IP话机、IP摄像头和打印机等哑终端由于不支持强认证方式（如802.1X、Portal等），且通常缺乏定时病毒查杀的机制，因此更容易成为被攻击和仿冒的对象。这些哑终端一旦被非法仿冒就很难发现，成为网络中的安全隐患，对业务构成威胁。

» **挑战2–接入方式多样化，网络私接带来安全隐患**

海量终端接入，除了传统的有线接入外，无线接入方式也越来越普及。同时，移动办公的兴起，员工和访客可能通过不同的网络接入点（AP）和交换机接入网络。当有用户未经授权私自接入网络（私接），会成为整个安全防御系统的最弱节点，大幅增加整网安全风险。私接设备可能携带恶意软件或病毒，对网络中的其他设备造成威胁。此外，私接设备未经安全加固，存在被黑客攻击的风险。黑客可以轻易通过这些设备侵入内网，窃取敏感信息或进行破坏活动。

5.2.3 华为终端安全无感接入技术，实现终端防仿冒、网络防私接

为了应对上述挑战，华为发布了终端识别无感接入技术，实现终端防仿冒网络防私接。

» **价值1–金融物联终端资产智能识别，仿冒终端高效检出**

在华为星河AI金融网点和园区网络方案中，华为防仿冒技术通过对终端流量特征的深度学习和识别，以及基于这些特征形成的流量行为模型。该技术通过实时监测和比对终端的流量行为，判断其是否符合正常行为模型，从而识别并隔离仿冒终端。

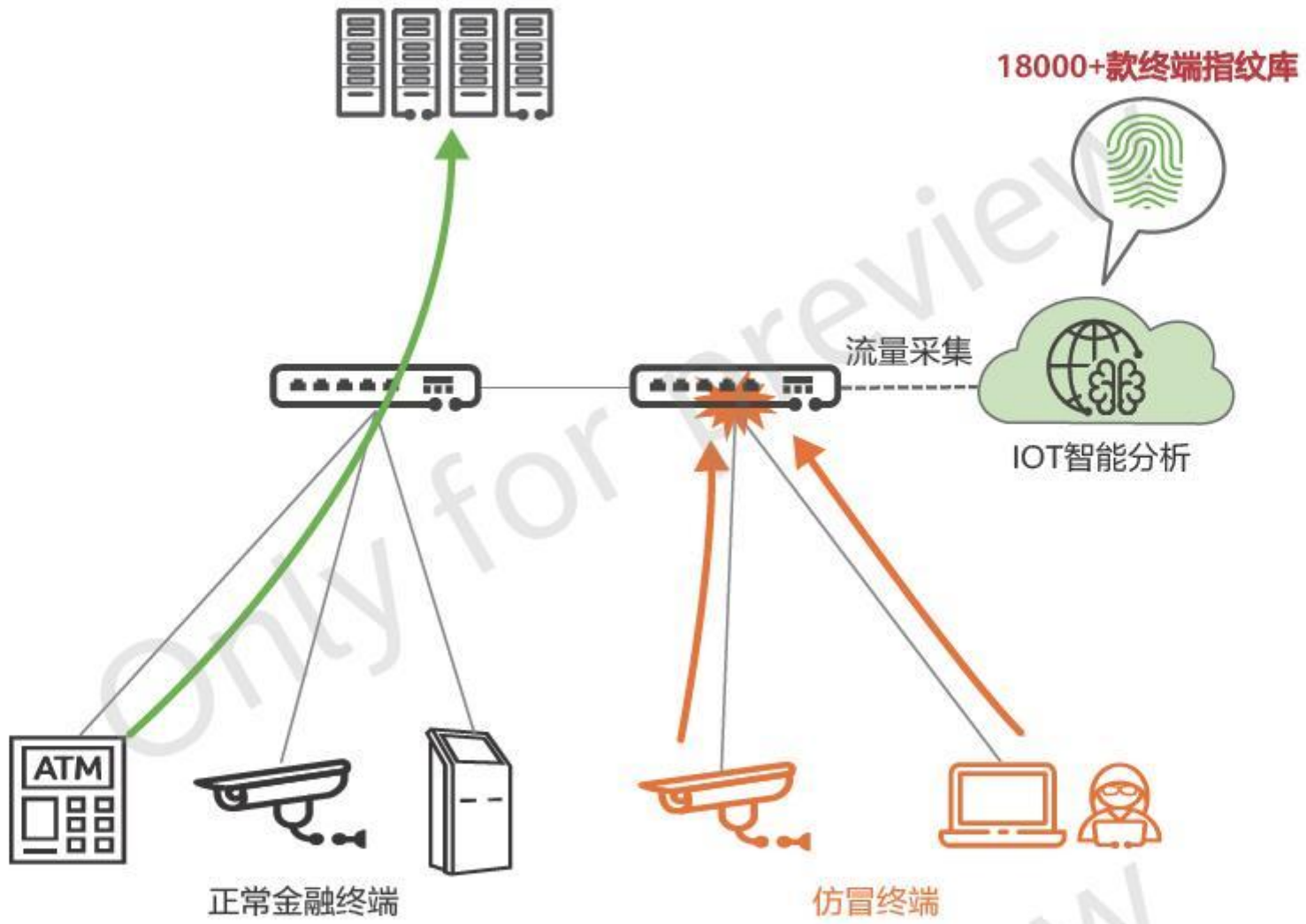


图5-2 识别并隔离仿冒终端

华为防仿冒技术通过学习和识别终端的流量特征，形成流量行为模型，构建终端指纹库，覆盖18000+款终端。哑终端（如IP话机、IP摄像头和打印机等）通常缺乏强认证方式和定时病毒查杀机制，容易成为仿冒目标，华为防仿冒技术能够特别针对哑终端进行防护，终端识别率超98%，有效防止仿冒终端接入网络，降低网络被攻击的风险，提升整体防御能力。

» **价值2-网络私接秒级检测与阻断，保障金融网络安全**

在华为星河AI金融网点和园区网络方案中，防私接技术旨在防止用户未经授权私自接入网络，从而保障网络的安全性和稳定性。该技术通过网络设备对终端报文的解析，结合MAC/IP信息以及HTTP、TCP、DNS报文中的特征字段，来判断用户是否存在私接行为。一旦检测到私接行为，网络会立即上报并采取相应的阻断措施。

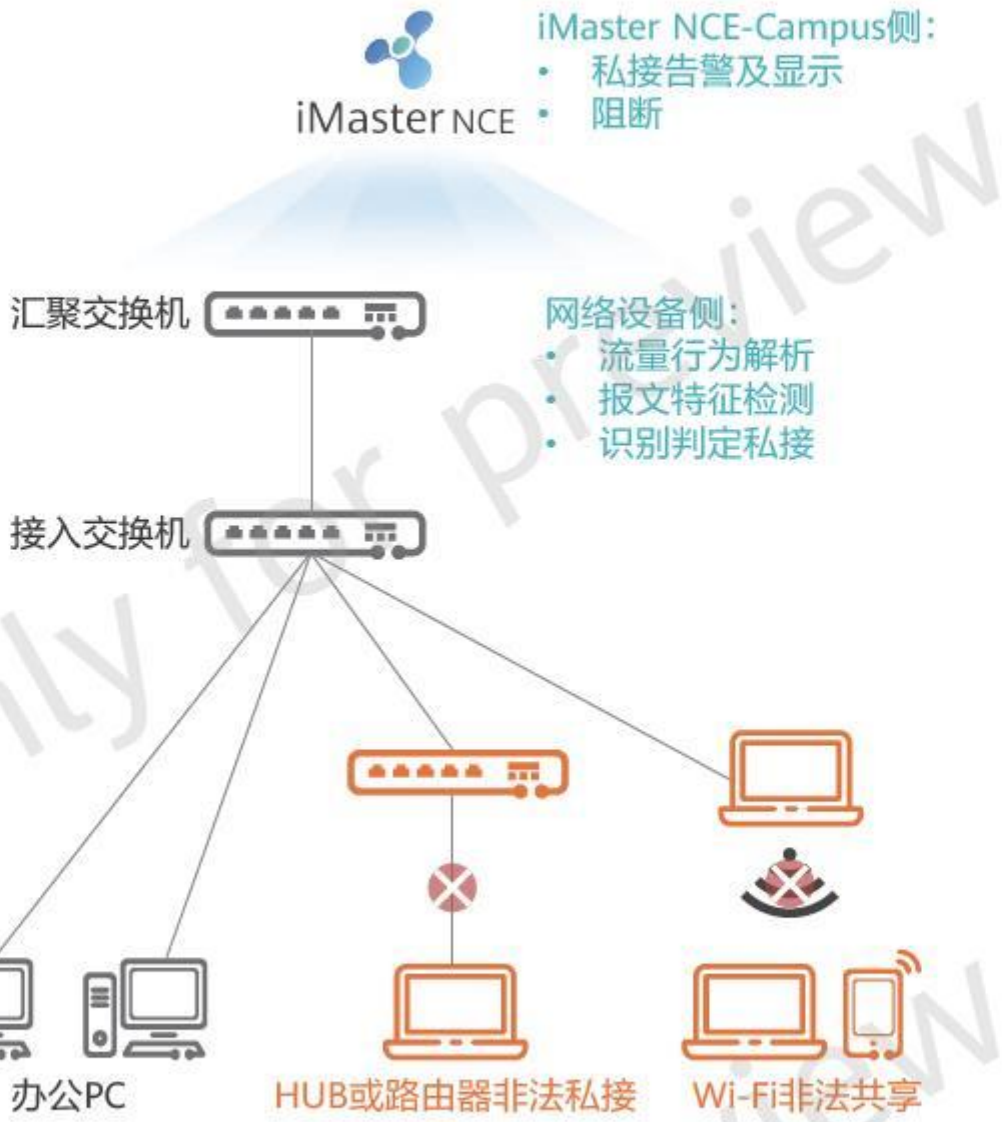


图5-3 网络防私接

华为防私接技术可实时自动化检测和秒级阻断未经授权的接入行为，有效防止了非法终端接入网络，从而降低了网络安全风险。这有助于保护客户的数据资产免受恶意攻击和非法访问。同时，整个过程无需人工干预，提高了网络运维效率。

5.2.4 成功案例：私接秒级检测与阻断，保障金融网络安全

某银行在例行审计时发现了异常交易记录，经过深入调查，最终发现这一事件是由一起网络私接行为引发的。该银行的一名IT部门员工A，利用自己的技术权限，绕过银行的安全监控，私自在银行内部网络中接入了一台非法设备。该设备能够捕获并转发网络中的数据包。通过该非法设备，员工A能够访问到银行客户的交易记录、账户信息等敏感数据。员工A利用窃取的信息，伪造客户身份，在银行交易系统中进行非法转账操作，将资金转移到自己控制的账户中。

由于网络私接行为的隐蔽性和复杂性，常规的网络运维管理难以察觉。该银行采用了华为的网络防私接技术方案，实时检测和精准阻断私接行为，有效防止了信息泄露、非法访问等安全隐患。

06 极致体验，打造场景化智能网点

6.1 金融服务嵌入到日常生活中，金融网点加速场景化转型

手机银行已成为金融客户业务办理的主要渠道，传统银行网点作为线下服务渠道，客流量、获客能力等均出现下降趋势，部分网点客户等待时间长，服务体验不佳，甚至引发客户投诉，造成客户流失。银行传统网点迫切需要通过技术创新来推进网点场景化转型。

国内大量银行纷纷尝试网点智能化转型，在网点中引入金融太空舱、智能柜员机、仿真机器人、家居银行、共享空间直播等应用场景，从客户旅程出发，重塑服务流程，实现手机银行、微信银行与网点的线上线下融合。通过智能的互动体验，让金融业务办理过程更具趣味性，大幅提升网点业务处理效率，减少排队时间，使客户享受便捷的服务与体验。据统计，网点智能化转型前后，客户满意度提升了20%，业务办理效率提高了30%。

6.2 海量智能设备引入，对业务体验和连接安全带来新的挑战

智能网点引入AIoT（Artificial Intelligence of Things，人工智能物联网）、移动通信等技术打造场景化服务，在提升网点金融服务体验的同时，也给网点带来了成倍的数据流量增长，银行网点对实时数据传输和大带宽的需求比以往任何时期都更加迫切。

国内网点采用的MSTP专线稳定性好，但带宽小（常见仅2M~10M）、成本高，难以满足琳琅满目的智慧应用的需求，同时网点还面临接入专线类型单一、容灾能力差以及物联安全管控弱等多个问题，智能网点转型对网络带来如下三点挑战：

» **挑战1-接入能力弱：网点智能化带来大量物联终端，对网络接入能力提出更大挑战**

随着智能以及移动设备的大量引进，在给消费者提供便利的同时，也带来了大量终端和移动接入诉求。近年来，国内许多大型银行快速推进智慧网点IoT战略，多家银行IoT设备接入总量已超千万台，银行亟需解决IoT设备高密接入问题。

» **挑战2-易窃听：引入无线网络后，需防止无线信号被窃听**

由于无线电传播的广播性质，无线空中接口是开放的，授权用户和非法用户均可接收到信号。黑客可通过无线空口窃取通信数据，再进行暴力破解。2022年某厂商的Portal页面遭到攻击，被植入了不当内容，引发了广泛的不良社会反响。网点中可能传输用户的账号密码等机密信息，必须保证数据的传输安全。

» **挑战3-体验差：金融网点承载多类生产和办公业务，业务体验保障要求高**

随着智慧网点的推进，很多网点对内上线了视频会议、OA、文件传输等系统，提升办公效率，对客户提供自助业务办理、AR/VR互动等智能业务，提升客户满意度。不同业务在传输过程中相互挤占网络资源，导致关键业务时断时续，用网体验差。

6.3 华为Wi-Fi 7和SD-WAN，支持终端高密安全接入、分支灵活互联、业务体验保障

为了满足金融行业网点业务连续性、物联接入安全性、业务体验有保障的诉求，华为提供 Wi-Fi 7、SD-WAN 等解决方案，提高网络接入容量、接入安全和接入体验。

» **价值1-华为领先业界一代无线终端Wi-Fi 7，将接入带宽和接入数量提升3-4倍**

Wi-Fi 7 作为新一代 Wi-Fi 产品，单射频带宽提升到 23Gbps，频宽从 160MHz 提升到 320MHz，调制方式从 1K QAM 提升到 4K QAM。Wi-Fi 7 的多 RU 技术解决了 Wi-Fi 6 信道资源浪费的问题，能够充分利用每一个“车道”传送信息，大幅提升并发率。Wi-Fi 7 还支持多链路同时上行，无线终端可同时使用 2.4GHz 和 5GHz 频段，让数据传输更快更可靠。下图为 Wi-Fi 7 相比 Wi-Fi 6 在带宽与并发性能上的提升。

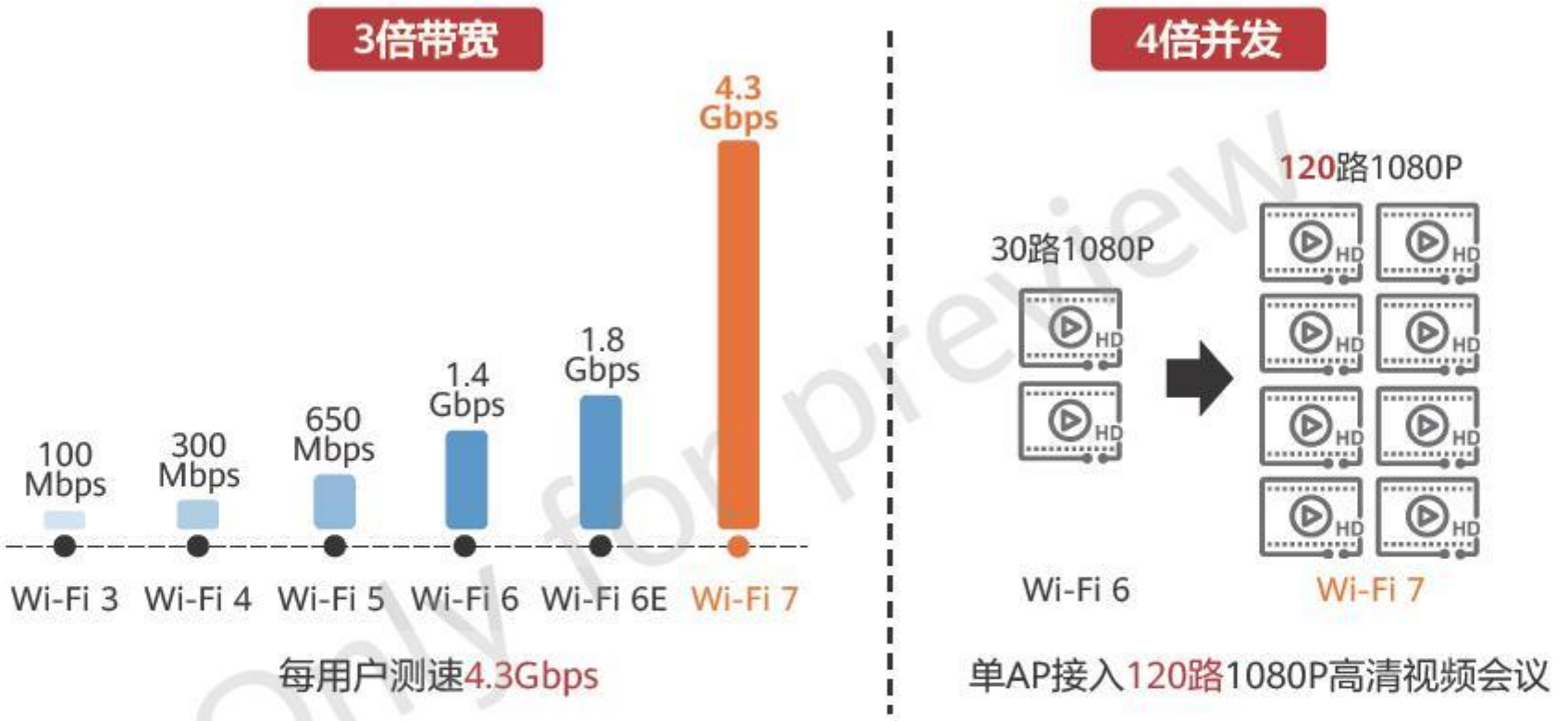


图6-1 Wi-Fi 7与Wi-Fi 6在带宽与并发性能上的对比

» **价值2-华为独家Wi-Fi密盾技术，有效杜绝无线窃听**

华为独家Wi-Fi密盾技术通过自研算法在物理层增加干扰，保障只有合法终端才能正确解析传输报文，非法终端只能收到包含主动干扰噪音的无效信息，不必担心信息被窃听。用户可以放心地将无线网络部署到网点、总部等生产和办公网络。

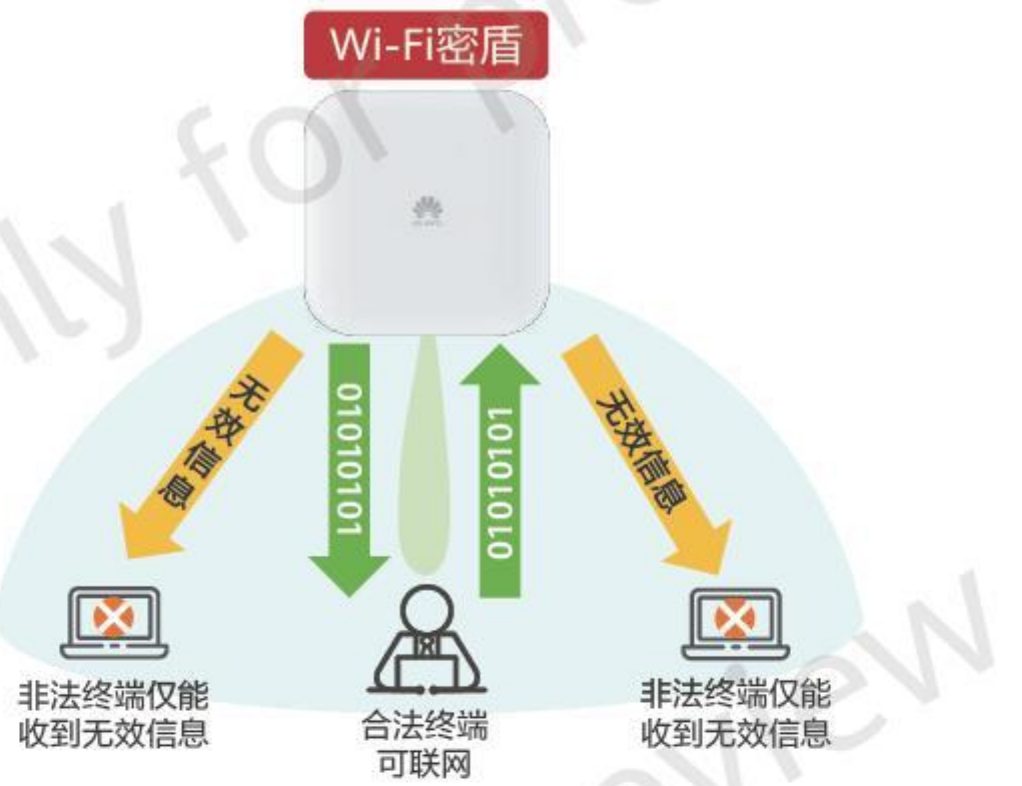


图6-2 华为独家Wi-Fi密盾技术

» **价值3-华为以应用体验为中心网络引擎，有效保障关键业务高品质传输**

针对带宽拥塞场景，华为推出 XNA（eXperience-centric Network Architecture，体验为中心网络架构）引擎，可智能识别网络中贪心流量（文件传输、软件更新等）并进行动态限流，优先放通视频等高优先级流量，从而保障拥塞场景视频会议依然没有卡顿。

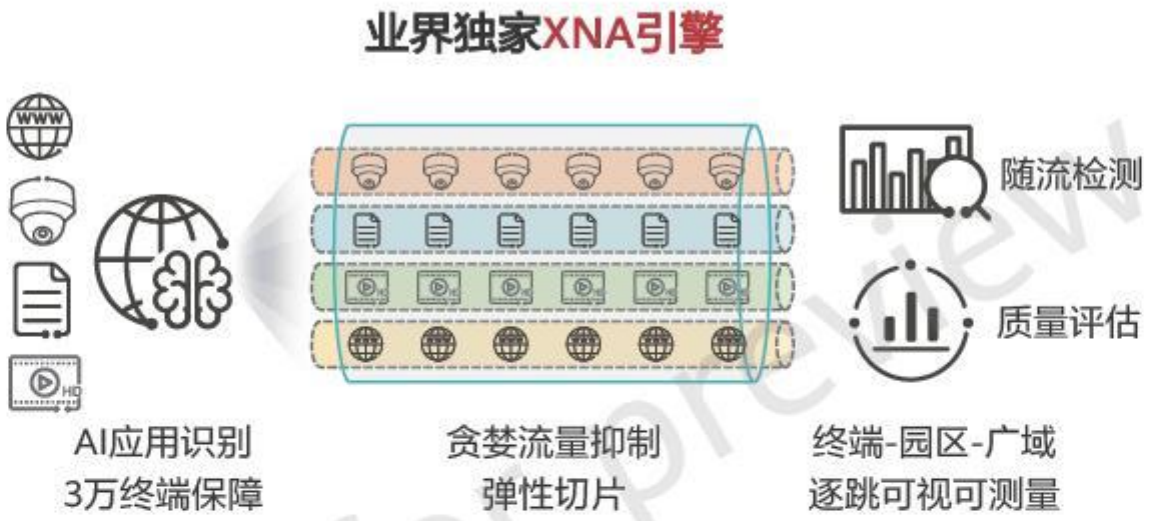


图6-3 华为XNA引擎

针对网络丢包场景，华为提供 A-FEC（Adaptive Forward Error Correction，自适应冗余前向纠错）技术，可基于网络丢包率智能增加冗余报文，在 30% 网络丢包的情况下，视频会议依然不花屏不卡顿，有效保障了视频会议的体验。

此外，华为支持基于 SLA、应用优先级、链路权重等多种流量调度算法，在保障高优先级业务体验的同时，可将广域链路利用率提升约 20%。

6.4 成功案例：华为高品质园区和智能SD-WAN方案，助力A银行打造面向数字时代的智慧网点

某头部银行计划实施网点智慧化改造，引入VTM（Virtual Teller Machine，虚拟柜员机）、机器人和IoT等新业务，以提升其市场竞争力。改造中发现网点主要存在两个问题：一是终端全部采用有线连接，不支持手持业务终端、机器人等移动产品接入，同时随着大量IoT设备的引入，网络布线成本陡增；二是广域接入全部使用专线，带宽低费用高，一台VTM需要10Mbit/s带宽，再加上安防、视频等业务，一年专线费用高达千万美元，但专线链路利用率却低于50%。

为解决上述问题，该银行选择部署华为高品质园区和智能SD-WAN解决方案，通过租赁一条10M的专线，加一条100M的Internet链路，替代租赁2条30M~50M的专线，在保障业务体验的同时，大大降低专线成本，一年节约400万美元：

- 部署华为Wi-Fi 7产品，有效解决接入终端密集、接入带宽不足等性能问题。
- 通过XNA技术优先传输音视频、交易等关键流量，并在拥塞时自动对文件传输等流量进行限速，确保关键业务体验。
- 通过SD-WAN智能调度确保核心业务跑在高品质线路上，非核心交易业务跑在Internet上。当专线出现异常或低于设定的SLA时，可快速将核心业务调度到Internet上。

07 写在最后

华为数据通信产品线一直以来秉承创新文化，坚持高强度的研发投入。2023年，我们在全球13个研发中心和17个技术Lab中已布局100多位科学家和顶级专家，长期从事前沿技术和产品的研究工作。

在这个充满机遇和挑战的时代，我们需要保持谦虚、勇敢和创新的精神，不断学习，不断追求卓越和进步。希望通过本书可以帮助大家了解金融行业的最新动态和趋势，更加深刻地理解数据通信产业在金融行业场景中的应用与价值。

数据通信产业还在快速发展中，受编写时间、编写经验等方面的限制，本书内容难免存在遗漏和不足，敬请广大读者批评和指正，您的宝贵意见是我们不断进步的动力。最后，需要特别感谢所有编写者所付出的心血与时间，让本书得以尽快付梓，在2024年热情如火的时节与大家见面。