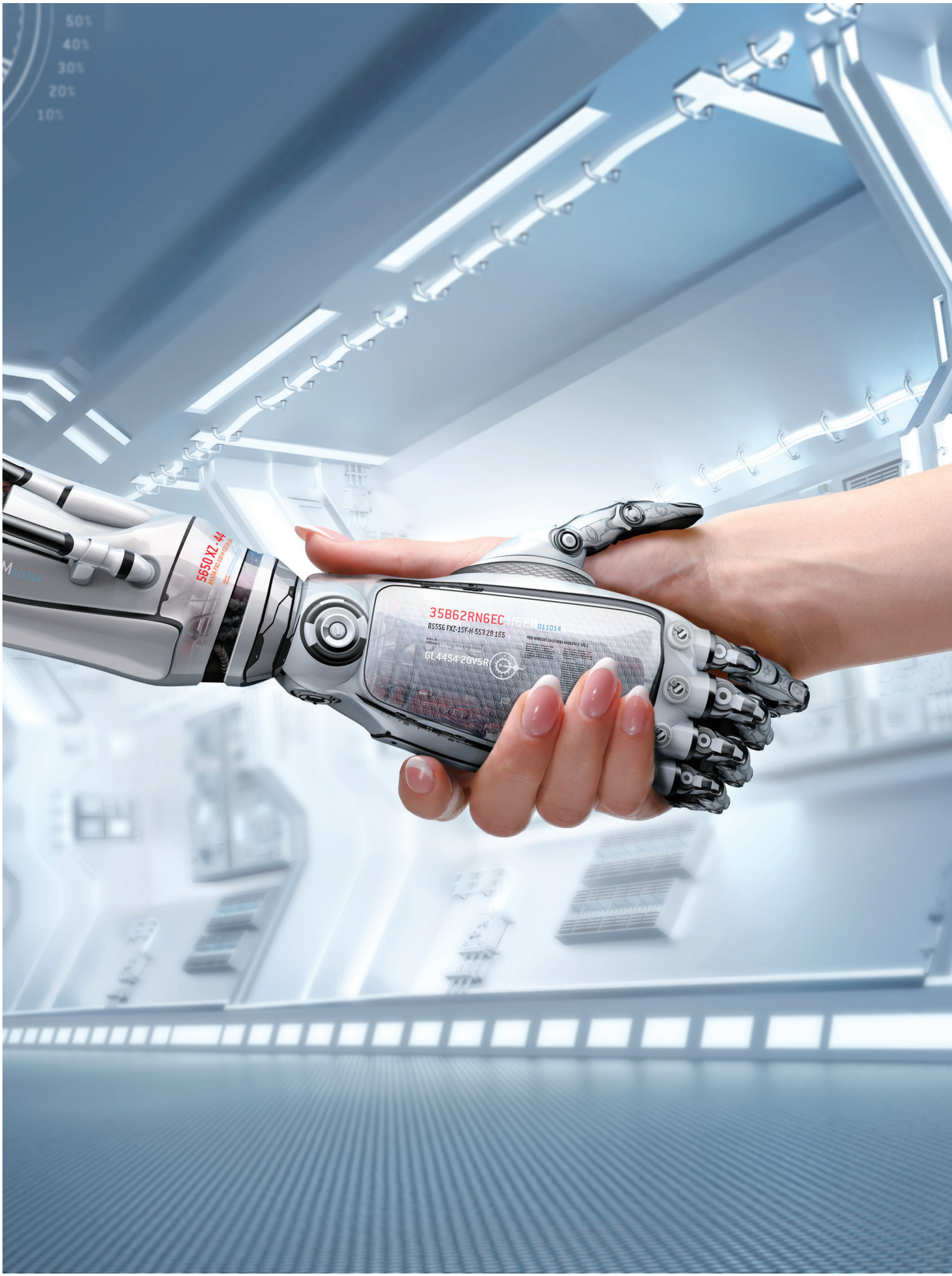
中国平安
保险·银行·投资

平安科技
PINGAN TECHNOLOGY

HUAWEI

SD-WAN在中国金融行业的创新实践


50%
40%
30%
20%
10%
5650XL.44
35B62RN6EC
85556 FXZ-15F-H-553 28 165
GL44S4 20V5R

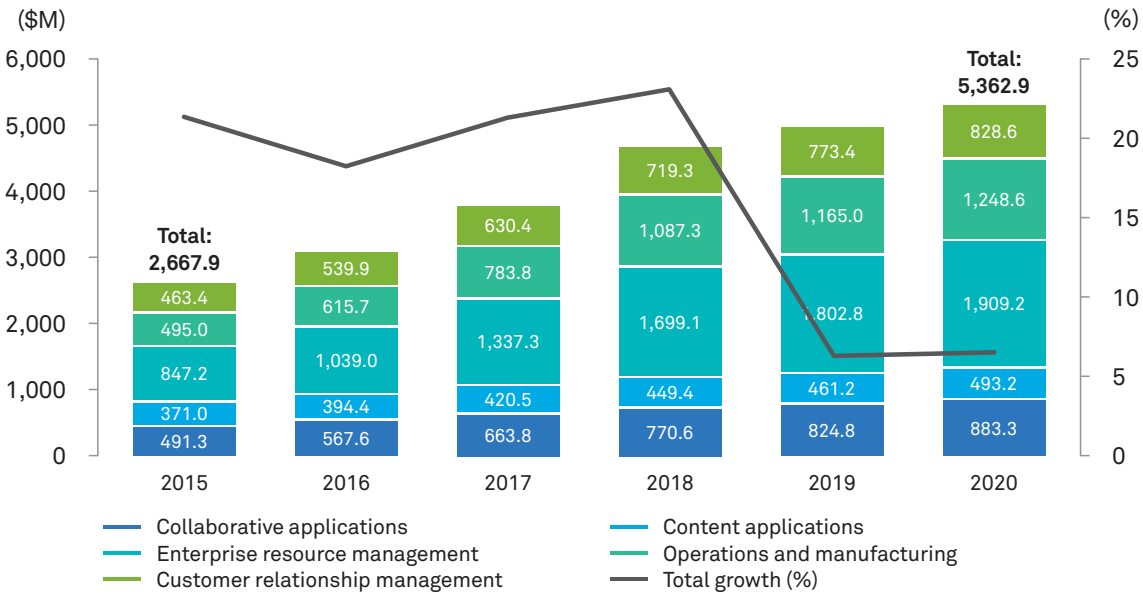
目录

01 SD-WAN的兴起

随着信息技术发展，数字经济早已成为全球经济的重要内容，是全球经济发展的主线，并在逐步推动产业界和全社会的数字化转型。

越来越多的企业系统和应用程序在云端部署，IDC预测到2018年超过一半的企业的IT基础设施和软件的投资是基于云的，到2020年这一比例将达到70%。越来越多的用户分布在更大范围的分支机构和其他地区，移动办公越来越广泛。在过去的十年中，企业的移动应用的数量和依赖于这些应用的用户的数量都得到了巨大的增长。IDC预测从2015~2020年全球企业移动应用收入的年复合增长率达到15.2%（如图1）。

Worldwide Mobile Enterprise Applications Revenue Growth



Source: IDC's Worldwide Mobile Enterprise Applications Forecast, 2016-2020: Mobile First, Mobile Only, Mobile Also (IDC #US40753716, September 2016)

图1 全球企业移动应用投资

企业业务的数字化和云化导致更多设备接入、用户的移动范围更广，给企业网络（包括广域网）流量快速增加，流量分布显著变化（穿越广域网流量显著增加）。企业网络面临的挑战是在于：灵活满足业务需求的同时不中断业务并提供更高的网络流量。随时随地、安全、可靠的访问企业系统和应用成为企业基本业务诉求。数字化企业的未来取决于是否能有效地应对这一挑战。

如何采用灵活的WAN架构来满足企业业务的诉求，是每个企业的CTO都在思考的问题。随着SDN/NFV、云计算、大数据、人工智能技术的成熟商用，宽带接入以及Internet骨干网容量和可靠性的持续提升（2017年Q4我国固定宽带平均下载速率达到19.01Mbit/s，相比2014年Q1增长510%），SD-WAN 应运而生。

2014年第一季度至本季度全国平均可用下载速率对比（单位：Mbit/s）

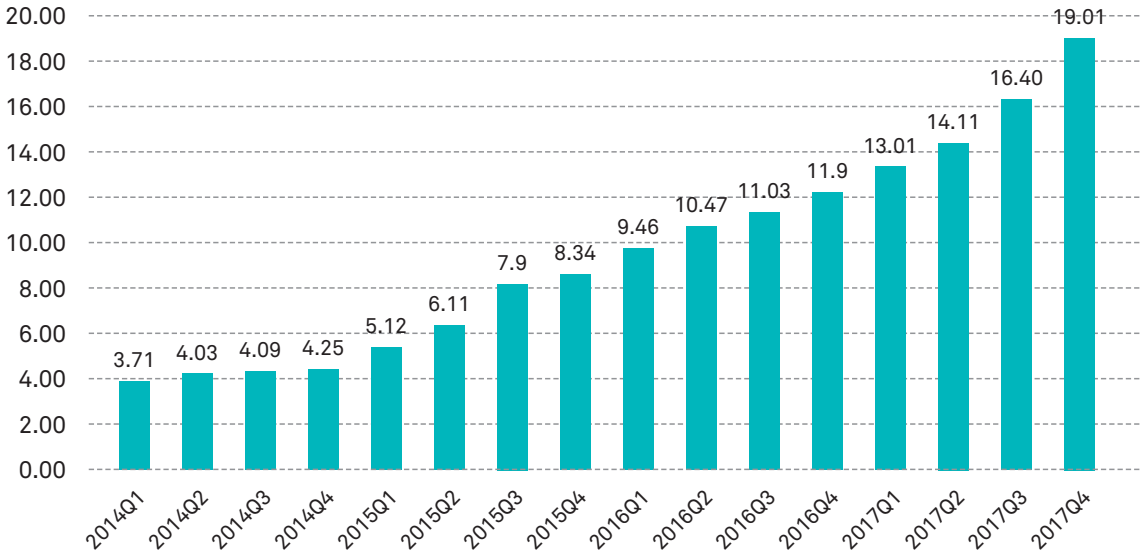


图2 中国宽带下载速率发展

SD-WAN不是凭空冒出来的新方案，仍然是根植在很多传统的传统企业级WAN技术之上的，主要包括路由、VPN、安全、WOC等等，并集成了SDN/NFV/云化等多种新技术，属于一揽子的解决方案。它包含硬件系统（如企业侧设备CPE），软件系统（如控制器）和服务、应用等多个部件，满足企业级广域网面向未来的性能、可靠性和安全性的要求。

硅谷从2011-2012年开始做SD-WAN，到现在也有6、7年了。最开始，SD-WAN在技术方案上是纯Overlay的，网络的连接和增值服务都在企业边缘设备完成，是面向企业自建自用的场景。大概从2016年开始，SP的角色开始被引入SD-WAN方案中，网络连接上要考虑对接SP的Underlay基础网络，增值服务方面要考虑对接SP的云。SD-WAN从技术实现和运营角色的不同分成2类方案：面向企业（Enterprise Oriented）的SD-WAN”和面向基础网络业务提供商（SP Oriented）的SD-WAN。

02 SD-WAN的应用

2.1 金融WAN的现状

金融行业作为国家经济的重要支撑，网点遍布全国。随着社交媒体以及移动技术发展，互联网金融业务在快速发展，传统金融的业务模式正在发生变革，金融业务种类极大丰富：除了传统的交易类业务，泛金融业务快速增加。传统以设备为中心的金融网络已经无法适应业务的发展，当前面临如下问题：

2.1.1 业务开通周期长，专线价格昂贵，业务灵活性差

传统企业应用部署在总部数据中心，并通过租用运营商专线将分支机构连接到数据中心（如图3所示）。通过运营商专线网络连接企业数据中心和分支机构。传统专线网络可获取性比较差，光纤/电路需要单独部署，耗费的周期长；专线跨越多个网络/运营商时，业务开通周期更长；并且，专线价格昂贵，业务不能够灵活订购。

图3 传统企业WAN网络

2.1.2 网络设备功能单一，业务扩展性差

几十年来，广域网（WAN）的发展都是在硬件方面不断提升网络的速率和容量，网络设备仍然大量使用单一功能单一硬件，功能扩展需要增加新的硬件设备，扩展性差，部署周期长。

2.1.3 无法适应云业务的发展

企业的IT基础设施和软件的投资已经开始向云迁移，云资源动态迁移、灵活扩展，对网络提出新的诉求：网络功能软件化，网络随着业务调整自动调整。传统的WAN架构以硬件设备为中心，已经无法适应云业务的发展。

2.1.4 网络管理方式低效，运维效率差

在过去的20年中，依靠CLI以硬件为中心的管理企业网络的方式一直不变。但随着企业业务流程变革和数字化进程的推进，云计算和移动互联网的快速发展，企业内部的应用和数据流量的分布已经发生变化，传统网络变得越来越不可预测、不安全且更加复杂。基于CLI的管理方式，配置效率低下，故障定位时间长。

2.2 金融SD-WAN的应用

金融是国家重要的经济命脉，金融机构是从事金融服务业有关的金融机构，是金融体系的一部分，金融业务包括银行、证券、保险、信托、基金等行业，金融机构也包括银行、证券公司、保险公司、信托投资公司和基金管理公司等。分散在全国的金融网点，通过广域网（WAN）实现网点互联和业务管理，SD-WAN在金融行业有广泛的网络基础和应用场景。

SD-WAN解决方案是一个开放、智能、分层的方案，从下往上包括联接层、云管理层、应用层三层（如图4）。

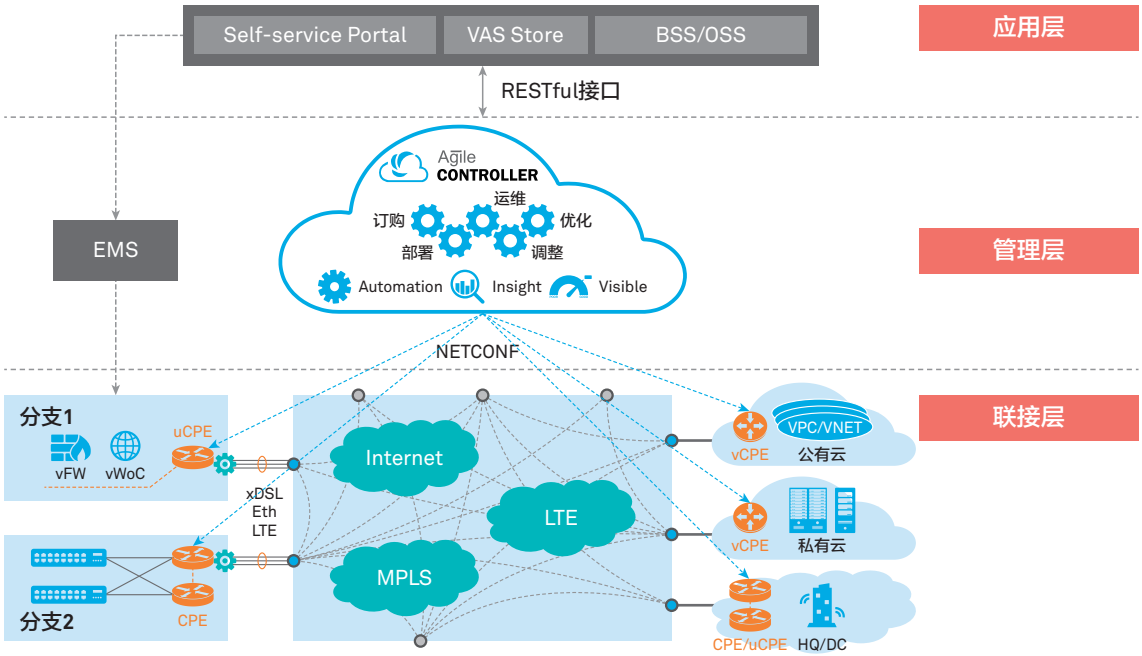


图4 SD-WAN整体架构

联接层是物理网络连接的基础，包含CPE、uCPE或者vCPE等软、硬件形态的网关设备，通过MPLS/Internet/ LTE技术建立连接，采用隧道技术构建Overlay网络。CPE：传统CPE设备，采用多核CPU和无阻碍转发架构，提供丰富路由和VPN功能。uCPE：基于NFV的通用计算平台，支持虚拟化功能，可安装第三方的VNFs。vCPE：虚拟CPE，可部署在KVM/FusionSphere/VMware虚拟化平台。

管理层是SD-WAN的中枢，是设备管理、网络管理、业务管理的核心。是基于SDN架构的管理控制系统，实现设备的统一管理，业务自动下发和Overlay网络的统一控制。南向通过协议和下层联接层设备对接，实现联接层设备和网络、业务的管理。北向通过开放接口与上层应用层实现对接，实现网络和应用之间的协同。

应用层是行业应用的具体实现，SD-WAN通过管理平台的Open API开放接口实现和应用层之间的数据开放和业务联动。

2.2.1 SD-WAN在金融大型网点的应用

金融行业营业网点是面向客户重要的窗口，是金融行业全业务办公的重要场所。传统网点业务以金融业务为主，业务相对单一，网络流量平稳可预测，传统业务对网络的诉求单一：高可靠性、高实时性、高安全性。传统金融营业网点到数据中心采用运营商提供的低速率、双专线组网实现业务数据的传输。

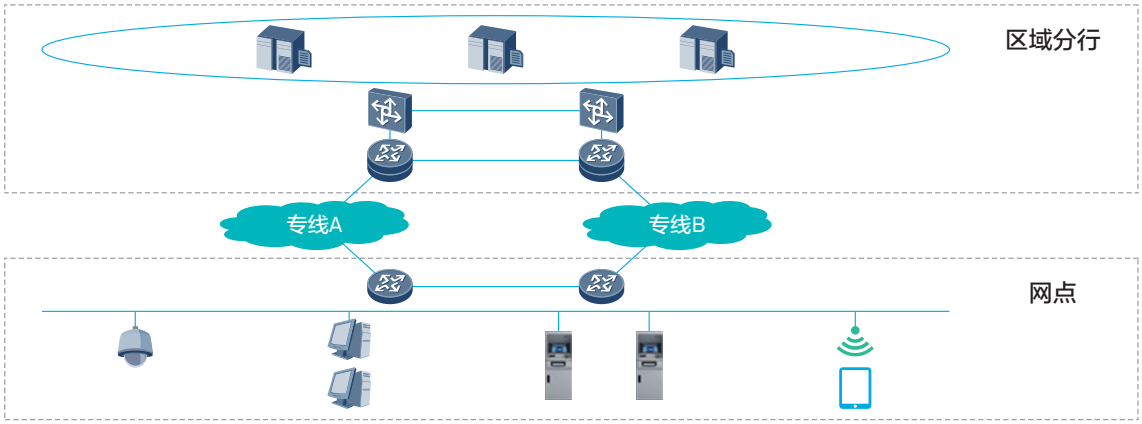


图5 传统金融营业网点组网

随着金融行业信息化、电子渠道发展以及业务创新对网点基础服务和交易功能的影响，传统交易和业务处理减少，“泛金融”服务增加。营业网点业务发生显著变化，种类增加：除了传统的交易数据业务，增加了非交易类的视频类、语音类、社交类业务。流量增加：传统交易类数据业务数据量小，非交易类的视频、语音、社交类流量大。

泛金融业务和传统交易类业务的叠加对金融行业网络产生了差异化诉求，传统网络已经无法满足。

	传统交易类业务	泛金融类业务
业务媒体类型	数据	视频、语音、大文件
业务流量	小	大
安全性要求	高	中
实时性	高	中
业务灵活性	长期不变	快速上线，灵活调整

面对金融行业网点对网络的差异化诉求，SD-WAN通过引入SDN/NFV/云化/大数据技术/自动化技术，打造了一张智能、开放、业务感知的金融网络。

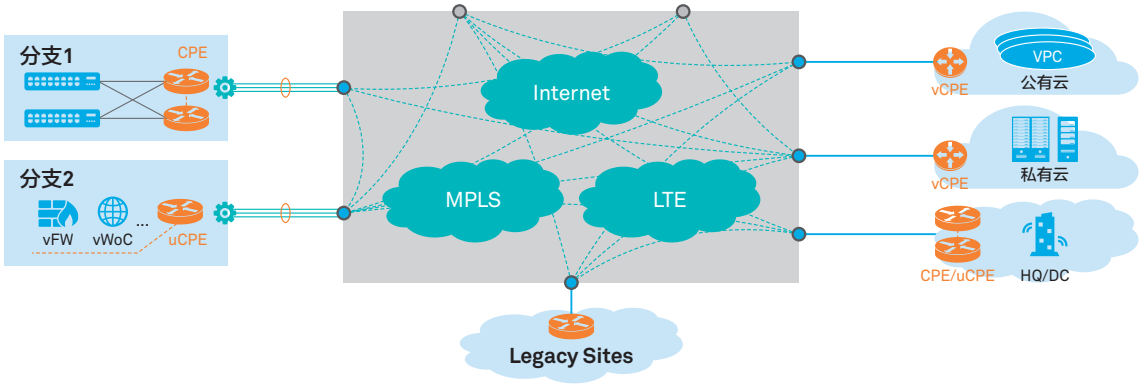


图6 金融营业网点SD-WAN组网

在大型网点和总部部署SD-WAN设备，数据中心集中部署控制器。SD-WAN设备识别传统交易类业务和泛金融类业务，针对业务要求选择最合适的传输链路，实现差异化服务。基于uCPE设备灵活部署网络业务，减少网点网络设备。vCPE在云端部署，支持业务灵活迁移。全网链路质量可视，及时发现网络故障和快速定障。WAN的端到端安全防护。

2.2.2 SD-WAN在金融分支网点的应用

随着国家普惠金融政策推动和金融行业自身业务发展（网点下沉：贴近客户、贴近社区）的需要，社区网点、流动网点、农村网点等小型网点数量激增。互联网金融和移动互联网金融业务的快速发展，远程语音、视频、人脸/声纹识别、机器人客服等新技术的应用，分布全国的小型用户服务中心网点急剧增加。

面对数量巨大、异构接入（光纤/网线/XDSL线路/LTE）、跨越多个运营商网络（电信/联通/移动）、网点分散单独金融小分支网点，如何打造一张适应业务发展，面向未来的网络保证网点业务的快速开通、业务的安全稳定、网络的可靠运行、简易运维，传统企业WAN技术已经力不从心，SD-WAN可以很好的解决这些问题。

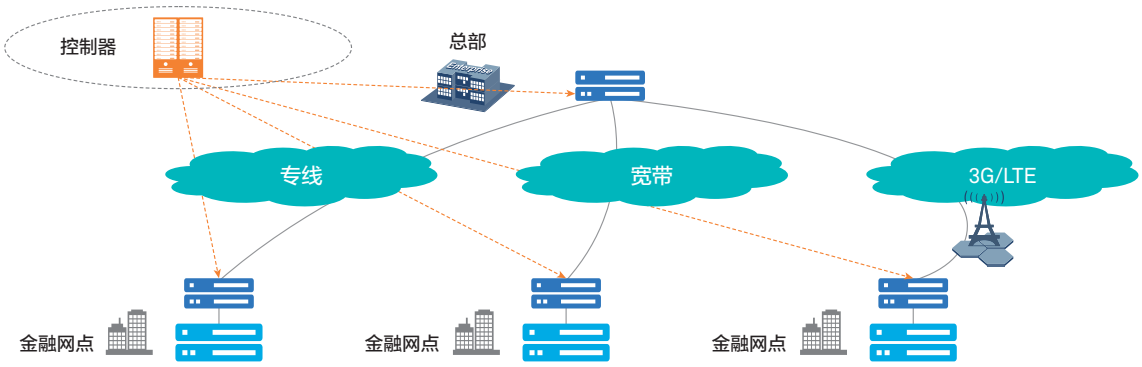


图7 金融分支网点SD-WAN组网

在分支网点和总部部署SD-WAN设备，数据中心集中部署控制器，实现分支网点设备的异构网络接入，ZTP开局，业务的集中配置，分支和总部WAN的链路质量可视，WAN的端到端安全防护。

2.3 金融SD-WAN的价值

SD-WAN解决方案提供的四大能力：①基于业务的多链路的选路；②连接+虚拟化应用统一部署和管理；③物理分支和云分支（私有云、公有云）融合组网；④海量分支集中管理、控制，面向有大量业务网点的金融行业有巨大的应用价值。

2.3.1 灵活业务

交易类和泛金融业务网络差异化服务保证：通过报文特征的深度识别技术区分交易类业务和泛金融业务，针对提供差异化服务，交易类业务优先保证，泛金融大带宽业务卸载到互联网承载降低网络接入费用。

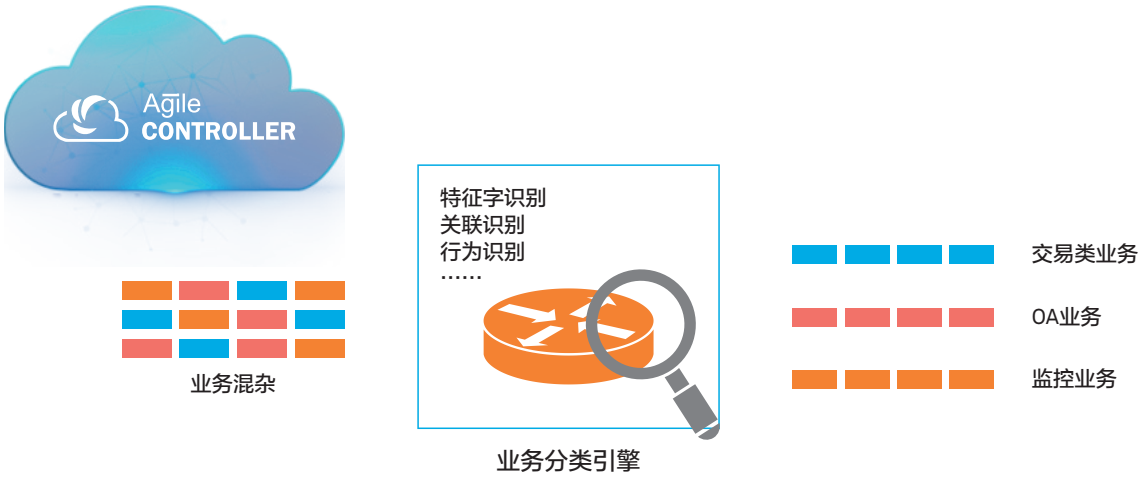


图8 交易类和泛金融业务区分

网络功能按需部署、动态调整：基于开放、虚拟化的uCPE平台灵活部署软化的安全、加速等网络功能，减少传统网络功能需要增加硬件设备导致部署周期长、网点网络复杂的困难。

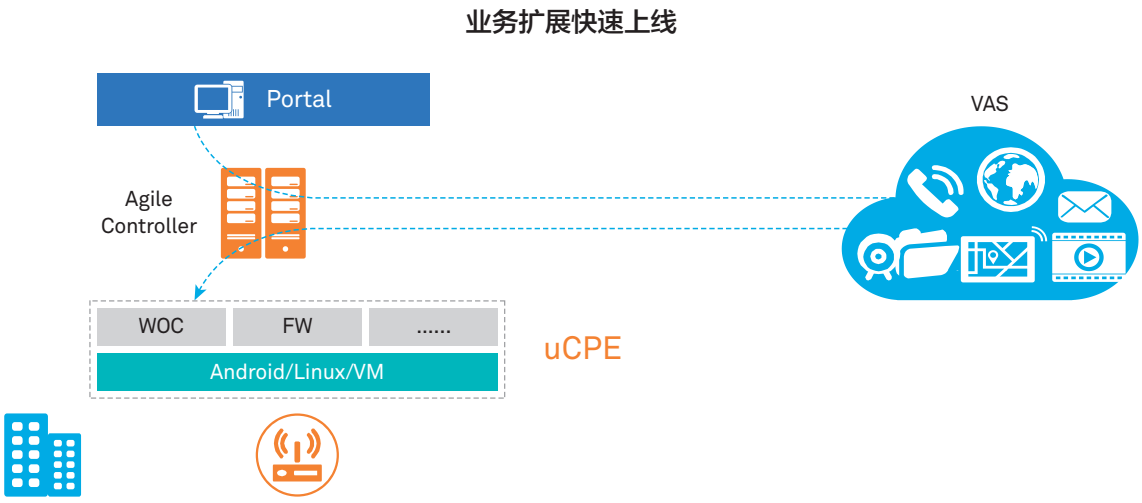


图9 网络功能动态部署

可靠：设备级+网络级双重备份，保障金融网络可靠。支持网点/数据中心侧双设备组网，网点有线和LTE的备份。

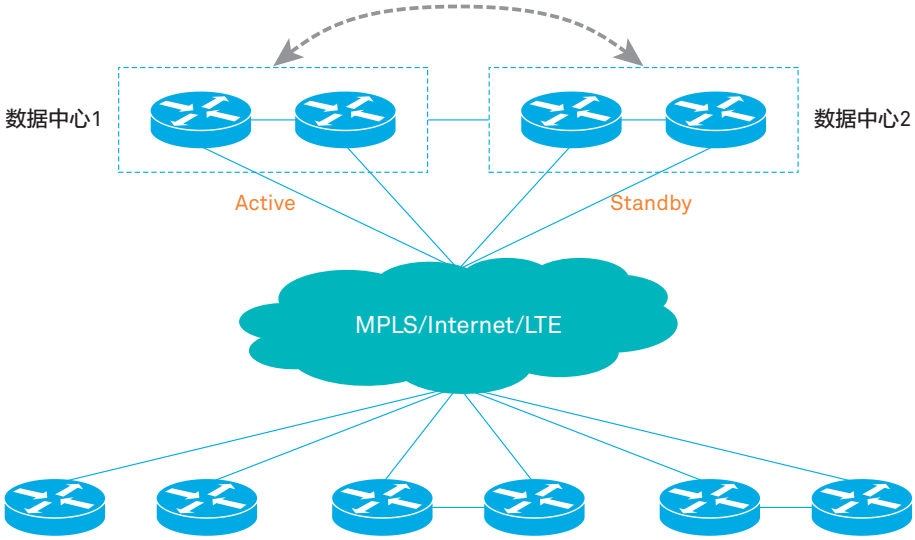


图10 设备/网络可靠保障

2.3.2 智能运维

快速开通：无IT背景人员现场，设备即插即用，业务快速开通，减少专业运维人员到场的费用；

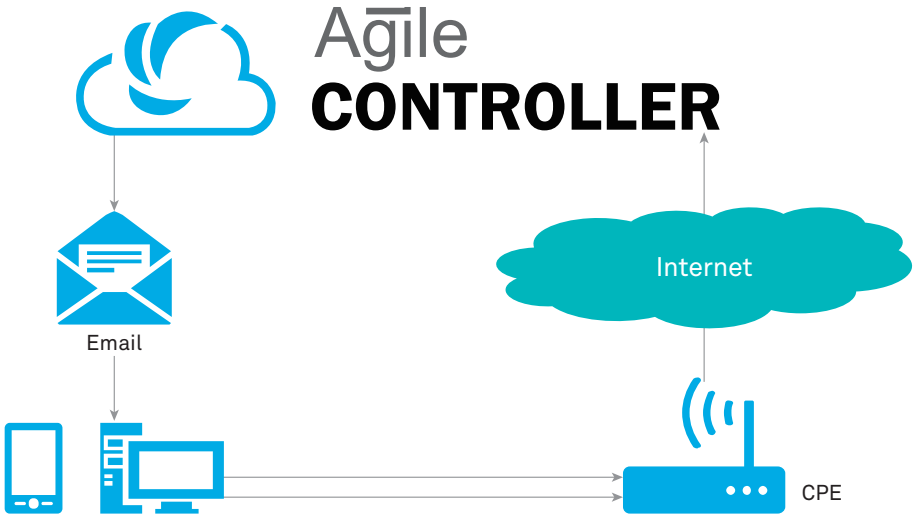


图11 网络快速开通

简易运维：利用自动化技术实现设备/网络的拖拽式、模板式、向导式配置；利用可视化技术实现设备、网络状态的可视化呈现，网络故障实时呈现，一目了然。

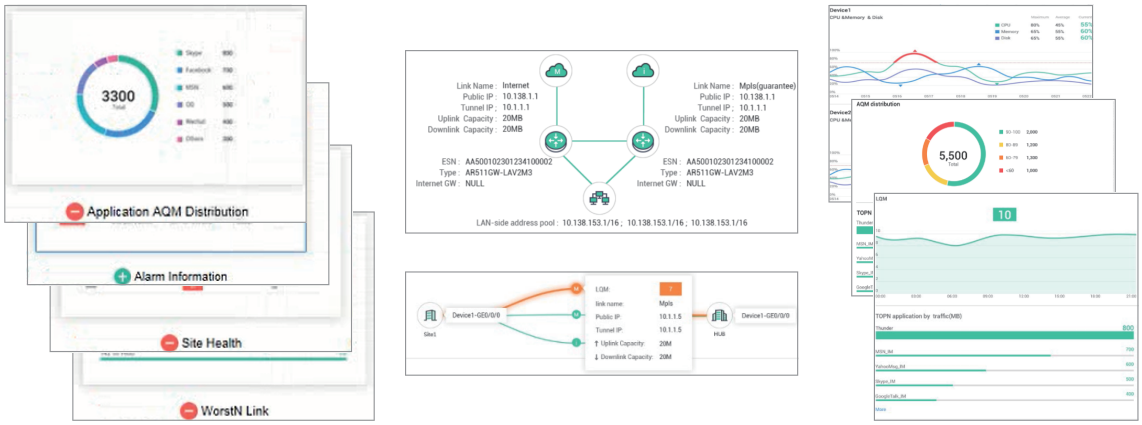


图12 可视化运维

2.3.3 安全合规

安全：管理平台集中管理整网安全策略，实现端到端、全方位网络安全。从网点设备接入认证、用户接入认证、设备防攻击、用户访问网络权限控制、网点到数据中心隧道加密传输、管理平台自身安全防护到管理平台的权限管理打造立体防护网。

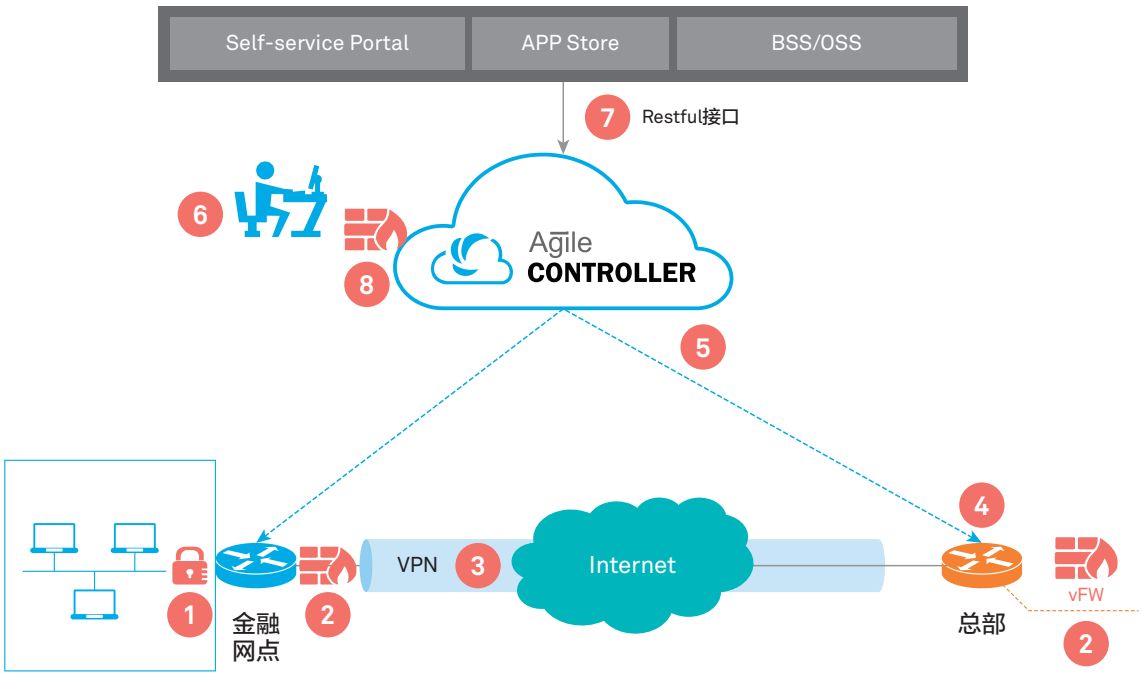


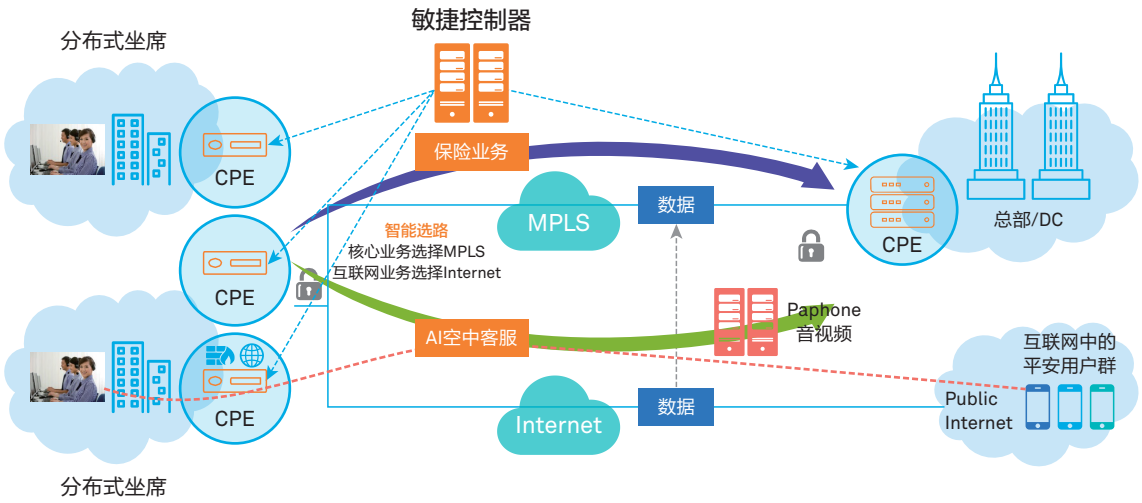
图13 端到端网络安全

03 平安SD-WAN实践

2017年中，平安首次在业内推出AI客服业务。AI客服让用户可以利用APP，从各地远程接入平安数据中心，系统通过人脸、声纹等生物认证技术和大数据匹配，远程核实客户身份信息，再基于客户地理位置，调配本地门店客服资源对话，实现“在线一次性业务办理”。

平安从业务支撑，快速交付，优化成本等角度出发，在保留原有私有专线的基础上，在AI客服项目中创新性的应用了全球首家规模化部署SD-WAN解决方案，开创了行业实践的先河。

业界领先SD-WAN解决方案，灵活、快捷的业务自动化系统



借力Internet	应用可视，智能选路	ZTP开局，智能运维	架构网格化
每年宽带节约1600万以上	业务灵活调整，区分服务	大幅降低人力和运维成本	就近接入，提升客户体验

图14 平安SD-WAN实践

3.1 灵活接入，优化成本

平安SD-WAN解决方案采用混合链路组网，4G/LTE、MPLS专线、xDSL等可任意组合，根据业务需求灵活定义业务流路径，并可根据业务需求弹性开通，快速切换，构建专线级的品质体验，并显著降低成本。

3.2 快速部署，集中管控

不需专业工程师上门，平安机构业务人员通过邮件开局快速部署，线路到位后20分钟之内即可完成一个分支的接入工作。

运维人员通过部署在数据中心的集中控制器管理各分支分布和接入情况，网络可视化效果带来人性化的全局视角体验。并可进行一点式批量维护升级设备软体、诊断网络故障。

3.3 开放接口，生态平台

在平安SD-WAN解决方案中，提供了丰富的API接口、开发编程工具以及丰富的行业应用的生态平台。可以根据业务需要，通过VM镜像直接加载流量控制，应用加速，CDN，安全识别等应用场景和业务逻辑。

3.4 云网融合，安全协同

平安SD-WAN解决方案将整合平安的LAN网络、WAN网络，数据中心网络、应用服务器、私有云、公有云等IT基础设施，不断增强网络+云+应用的整体协同，实现面向业务的端到端网络在线开通，网络随业务调整自动调整。最终云、网络及应用变成有机的一体。

为了确保分支机构和广域网免受越来越复杂的威胁，SD-WAN平台使用高级威胁检测技术的嵌入式的安全功能。平安SD-WAN解决方案将整合更全面的安全性、广域网优化、虚拟化功能到一个平台中。

缩略语

术语	解释	中文
WAN	Wide Area Network	广域网
ISDN	Integrated Services Digital Network	综合业务数字网
MPLS	Multi-Protocol Label Switching	多协议标记交换
CLI	Command Line Interface	命令行接口
SDH	Synchronous Digital Hierarchy	同步数字体系
OTN	Optical Transmission Network	广传输网
Ethernet	Ethernet	以太网络
SLA	Service Level Agreement	服务水平协议
SD-WAN	Software-defined networking in a wide area network	软件定义广域网
E2E	End-to-end	端到端
SDN/NFV	Software-Defined Networking & Network Functions Virtualization	软件定义网络和网络功能虚拟化
SaaS	Software as a Service	软件即服务
Agile Controller	Agile Controller	敏捷控制器
DSVPN	Dynamic Smart VPN	动态智能VPN
VRF	Virtual Routing and Forwarding	虚拟路由转发
HQoS	Hierarchical Quality of Service	分层质量服务
ISP	Internet Service Provider	服务提供商
CPE	Customer Premises Equipment	客户端设备
uCPE	Universal Customer Premises Equipment	通用客户端设备
vCPE	Virtual Customer Premises Equipment	虚拟客户端设备
ZTP	Zero Touch Provisioning	零接触部署

商标声明

 、**HUAWEI**、**华为**、  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。华为可能不经通知修改上述信息，恕不另行通知。

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