面向服务可保证的工业互联网网络切片

中国移动研究院

网络改造技术篇/前沿技术/工厂外网改造

1 概述

1.1 背景

工业互联网浪潮下，IT、CT 和 OT 技术已经出现深度融合的趋势。IT 需向 OT 注入敏捷灵活的业务应用，例如工厂网络如今普遍引入 MES、SCADA 等工业软件系统；工业生产流程正在向数字化与信息化发展；基于大数据的人工智能以及预测性分析也得到了越来越广泛的应用。CT 向 OT 注入可靠可管的网络服务，例如 CT 需满足工业网络有线或无线等接入方式的多元化需求；需要 SDN 技术实现网络灵活调度集中优化；需要 NFV 技术实现网络设备资源共享和多生态应用等，以保障低时延、高可靠、确定性的工业内外网络承载。

在垂直行业的多样化需求的促使下，运营商需要提供端到端的全方位服务。一方面，不同垂直行业存在多样化的网络接入方式以及协议标准。另一方面，不同的业务也对组网有着差异化的需求，例如 VxLAN、L2TP 等的各类隧需求、苛刻的端到端网络时延需求、极高的安全性及数据隐私保护需求和端到端的贷款保障与定制化 QoS 需求。在新型的网络需求背景下，运营商需化“管”

为“保”，提供服务质量可保障的能力，张弛有度地经营共赢生态，促进行业健康有序发展。

1.2 实施目标

网络切片是从运营商网络中划分出的一部分基础设施资源以及网络/业务功能实体形成的虚拟网络及资源池。面向服务可保证的工业互联网网络切片解决方案可以为垂直行业用户提供连接、带宽、时延、安全、管理、可靠性等多样化的网络定制服务。

1.3 适用范围

本方案利用网络各层的物理和逻辑隔离技术来划分网络资源，为垂直行业提供质量可保障的基础网络服务，适用于各个垂直行业以及对网络质量有特殊需求的场景，例如低时延以及确定性时延的工业运动控制场景、企业各分部之间高安全需求的专线场景以及组网方式灵活可变的柔性制造场景等。

1.4 在工业互联网网络体系架构中的位置

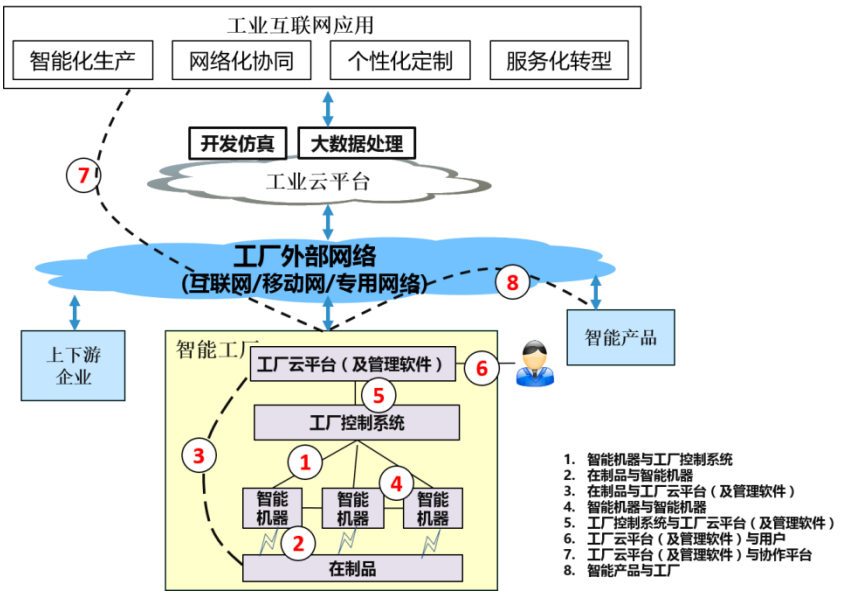

图 1 工业互联网互联示意图

本解决方案主要涉及工业互联网体系架构中的工厂外部网络（互联网/移动网/专用网络），并涉及多方面的业务流程，例如，工厂云平台与协作平台、智能产品与工厂之间数据的安全传输问题；也可应用于智能工厂内部网络，例如智能机器与工厂控制系统的交互、智能机器之间的交互、工厂控制系统与工厂云平台交互的实时性以及可靠性问题。

2 需求分析

2.1 业务端到端时延可保证

传统业务聚焦带宽保证，现阶段承载网通过建设专网、流量优化调度和及时扩容的手段，满足业务对带宽的需求。在较高的带宽需求之外，新型业务为给用户提供极致的业务体验，对网络端到端的时延也提出了新的需求，包括了极低时延和确定性时延两方面。

极低时延需求是对时延的绝对值进行优化，从数十毫秒提高到数毫秒，已经成为 IP 承载网未来技术演进的重要需求之一 。在车联网、远程医疗等极端业务场景中，时延要求达到 1 毫秒以下，否则业务将无法正常运行，从而带来一系列安全性等问题。

确定性时延针对时延标准差进行优化，是端到端时延敏感型业务质量衡量的新维度，也对网络承载技术提出了更高的要求。工业控制、远程医疗、机器人等应用领域需要控制信令端到端精准的传输，例如多机械手臂联动、柔性制造，人机互动等场景下，

确定性时延是多个控制系统协作的基础。

工业互联网网络发展的目标是低时延+高确定性，不仅要实现及时性，更要实现准时性。时延指标无法用设备转发能力的堆叠实现，而是需要从设备转发面、控制面的实时性，设备部署位置等维度综合考虑和优化，这将是下一代承载网面临的重要挑战和技术难题之一。

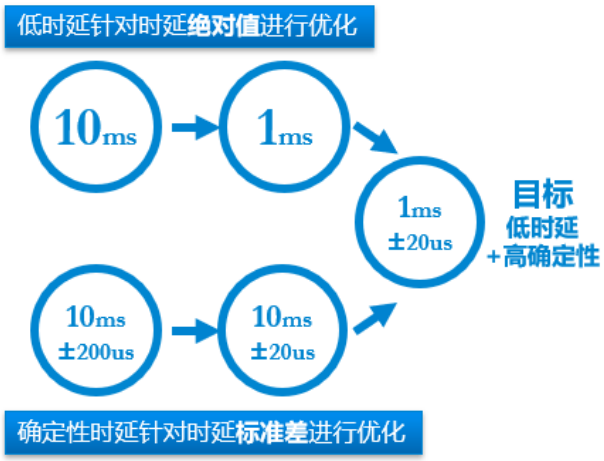

图 2 工业互联网网络时延优化目标

2.2 泛在的计算及存储资源改变流量模型

集中式 DC 部署呈现汇聚式流量模型，以主机为请求对象效率最高，流量的疏导和优化在汇聚式流量模型中呈现一定规律性，较为容易疏导。

泛在的边缘计算促使流量模型离散化，泛在的计算/存储资源是满足未来业务极致体验的必然发展方向，流量模型更加扁平化、离散化；以信息为请求对象（ICN）有利于提高网络使用效率。

网络切片可以在提供专用网络连接资源的同时，也提供定制

化的相应的计算和存储资源，以满足泛在计算新型的流量模型。

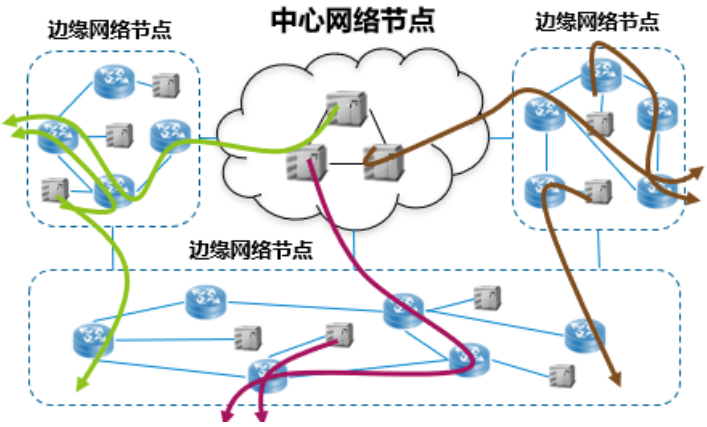

图 3 扁平、离散式的流量模型

2.3 网络及数据的安全

工业互联网的趋势下，工厂内网需要 IP 化进行互联互通，部分数据会上传至云端进行数据分析等。工厂网络互联互通为生产制造全流程自动化提供了网络基础，云网互联为大数据分析优化生产效率等提供了存储及计算资源，同时，也将会带来一定的安全风险。原本工厂层级化的组网模式可以使车间网络免受互联网攻击带来的影响，全网 IP 化为工厂全网以及各子网之间的安全性提出了更高的要求；工业数据上传至云端也带来了数据被窃取及篡改的风险，需要更加可靠和安全的专用网络传输机制也来保障工业数据的安全。

3 解决方案

3.1 方案介绍

网络切片是从运营商网络中划分出的一部分基础设施资源以及网络/业务功能实体形成的虚拟网络及资源池，满足垂直行业用户在连接、带宽、时延、安全、管理、可靠性等多样化定制

需求。

在传统网络“尽力而为”的传输方式下，多种业务流数据在网络中混合传输，相互干扰，无法确切保证某种业务流的传输需求，如图 4。网络切片可以将大网资源进行细粒度划分和专用，为不同业务提供定制化的保证能力，如同不同业务都在各自的“专网”上传输，互不干扰，具有专用性、异构性和灵活性等特点，如图 5。

专用性：网络切片实现网络资源的高隔离性来保证业务间的专用性，并可以提供带宽时延等指标的保证。

异构性：网络切片可以兼容承载网各管理域，形成全网络资源视图，实现端到端编排。

灵活性：网络切片具备随业务需求变化而灵活调整的能力，提供可定制的业务要求和体验。

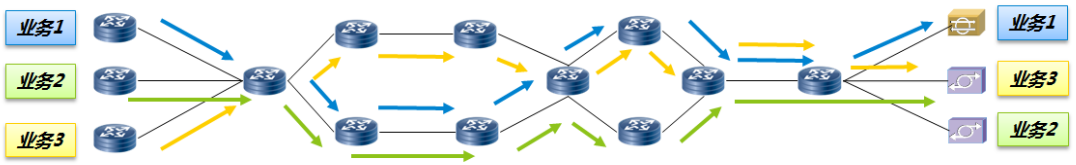

图 4 不同业务在传统网络中大多采用尽力而为的方式进行承载

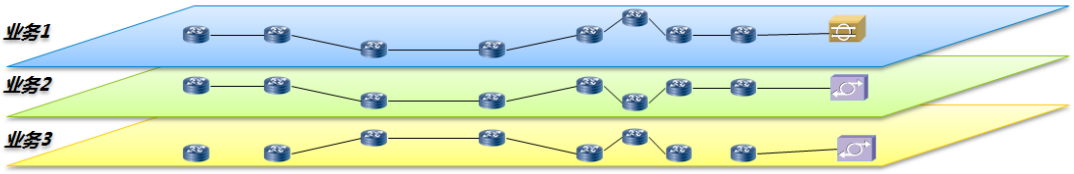

图 5 网络切片为不同业务提供隔离性强的定制化的保证能力

在网络切片服务中，运营商是典型的网络切片提供商，拥有网络基础资源及该资源上承载的各类网络/业务功能实体，基础

资源和实体是网络切片的组成元素；网络切片的租户可以是虚拟运营商、行业用户及个人用户。通过运营商的切片管理系统，租户可以根据自己对基础资源及网络/业务功能的要求申请定制化切片服务。

3.2 系统架构

系统架构包含了网络切片编排器（NSO）、可用的切片相关技术管理、底层网络资源和功能等部分，并且包含了网络配置模型（NCM）和设备配置模型（DCM）等模型。切片提供者将网络切片作为服务(NSaaS)传递给用户，但是往往用户可能需要不同的切片技术来实现相关功能，这就需要网络切片的编排器来协同异构的底层网络资源。

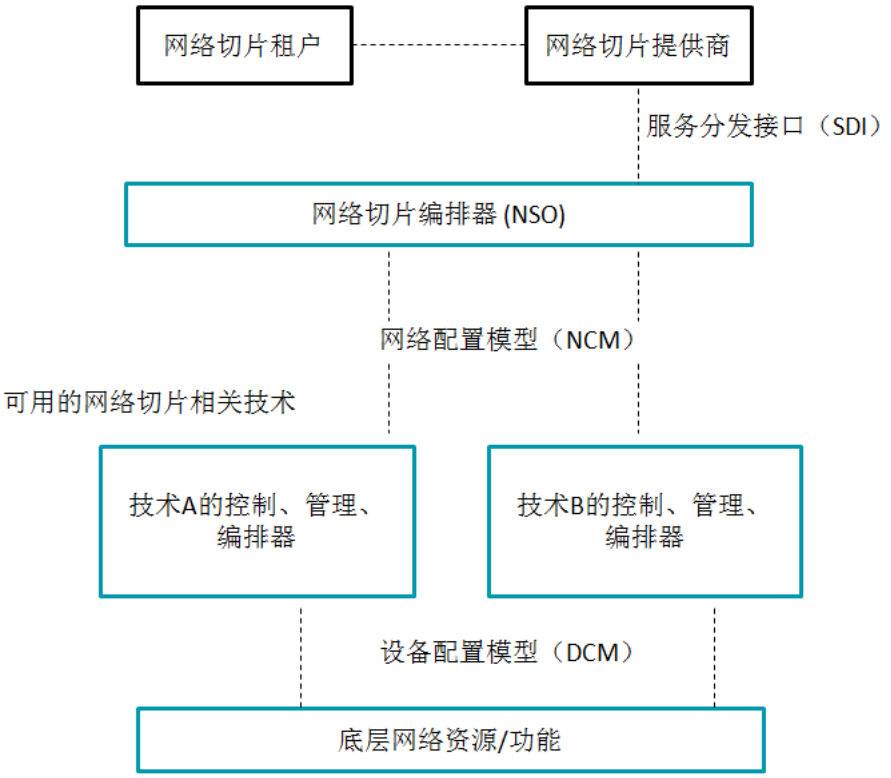

图 6 网络切片的编排架构

用户 NST 通过服务模型来请求 NSaaS,该服务模型用用户的语言来描述切片，通常为业务体验类的语言。切片提供者（运营商）将用户需求翻译给服务传递模型，这个模型可以用来描述运营商怎么使用自己的资源来提供支持业务。该传递业务模型会被发送到网络切片的编排器（NSO），并且和不同的技术来映射，进一步分解到网络配置模型中。最终在网络配置模型（NCM）中建立起相对应的底层设施和功能的参数，从而调用相应的底层资源建立起相应切片的服务。

3.3 网络拓扑设计

网络切片的建立及业务的访问流程如图 7 所示，主要包括参数映射、切片编排与分发、域管理控制等。参数映射模型提供将切片用户的业务需求映射为具体网络性能指标的依据，切片编排与分发器调用相应底层的连接与存储资源来实现不同指标网络切片的建立，域管理控制实现网络切片的跨域传输。

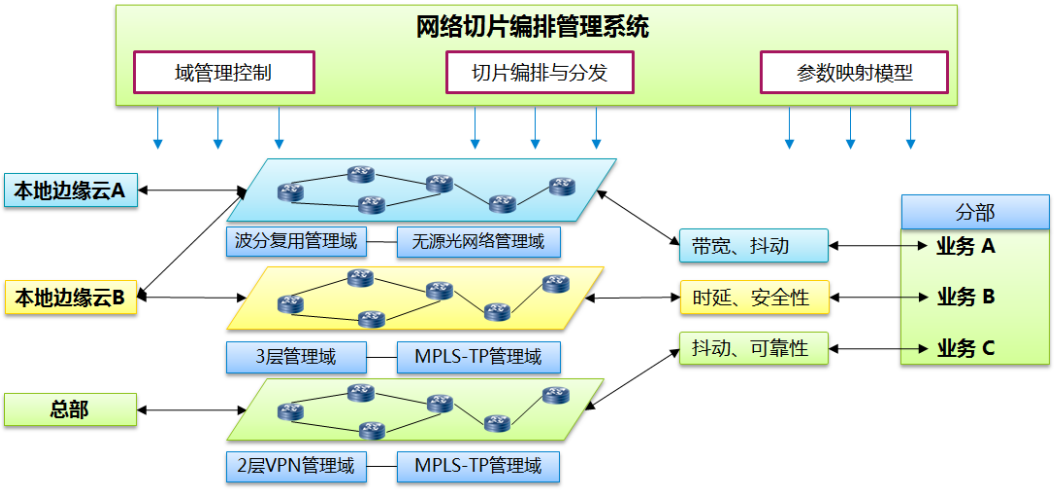

图 7 网络切片的建立及业务传输流程

3.4 功能设计

3.4.1网络切片的智能化配置

网络切片实施的关键步骤是将用户的实际需求映射为传统网络质量需求，例如将流畅清晰地播放视频和语音，实现网络设备的即插即用以及保障 7 天 24 小时随时在线等需求，映射为网络的平均峰值带宽、时延、抖动以及故障保护等指标，从而使网络切片提供商提供相应专用、隔离、服务可保证的网络切片。并且，可以引入 AI 技术实现参数映射和迭代优化，更好的满足用户需求。

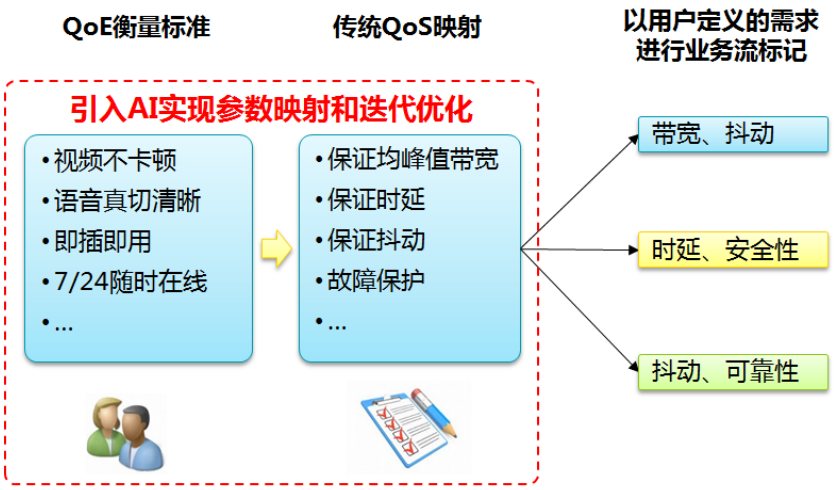

图 8 网络切片的智能化配置

3.4.2网络切片的跨域管理

跨管理域编排实现端到端的网络切片管理，满足不同网络拓扑、性能与功能的需求。网络数据的传输过程中，不同的业务会由不同的方式或不同的网络协议进行承载转发。例如，分支机构向总部的业务请求，可能会经过 2 层 VPN 到 3 层路由等协议，分支机构向云发送业务请求，可能会经过无源光网络到波分复用的转换等。网络切片需实现网络各层级转换的无缝衔接，保障业务

数据流端到端的可识别性，从而提供专属的网络切片来进行承载和转发。

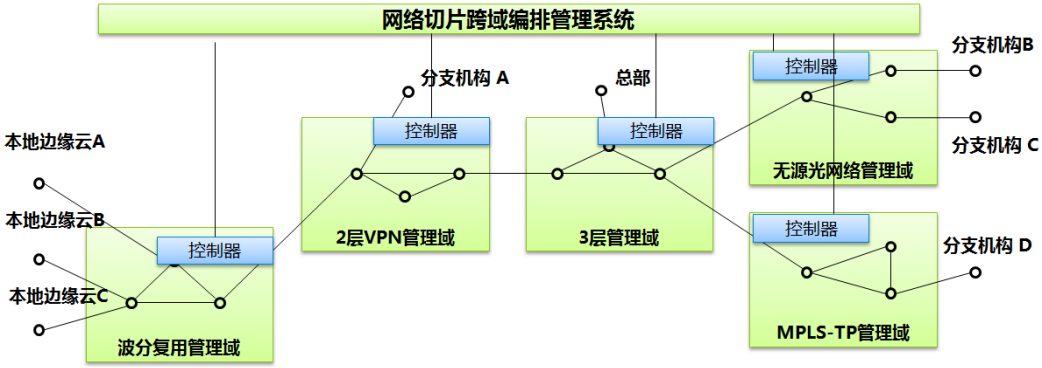

图 9 网络切片的跨域管理

3.4.3计算资源与连接资源统筹调度和编排

网络切片可以实现计算资源与连接资源统筹调度和编排，满足垂直行业需求的网络与计算资源一站式服务。传统模式下，用户需要分别向云服务提供者和互联网服务提供者请求 IaaS、PaaS、SaaS 服务以及 VPN、CDN 等网络服务。网络切片可以通过仲裁服务商提供给用户集成式一体化的端到端的服务。

图 10 网络切片提供一站式服务

3.5 安全及可靠性

网络切片技术的安全和可靠性在业界还有待讨论，但网络切片解决方案可以在一定程度的保障业务的安全性。网络切片将网络各层资源进行物理和逻辑上的划分，具有非常强的隔离性，各切片之间共享物理网络通道但互不干扰，某一条或几条业务流的

传输失败或某个网络切片的传输异常不会对其他切片和业务造成影响,保障了业务的可靠性。同时,网络切片还可以利用加密、隧道协议等技术来保证业务流的传输安全性,避免数据被窃取识别,保障了业务的安全性。