HUAWEI | CAICT 中国信通院 | Parametrix.ai 超参数 | Glodon 广联达 | Quwan 趣丸 | 北京大学 PEKING UNIVERSITY | 中国科学技术大学 University of Science and Technology of China

# 全域互联　一键贯通

## 企业级骨干网云化演进趋势解析

# 编制组 | Compilation Group

华为云计算技术有限公司：

赵海飞、郜忠华、王晓妍、李国帅、陈高翔、潘辰、朱兴骅、王少岩、林功元

中国信息通信研究院云计算与大数据研究所：

雷　昊、周丹颖、刘如明、李祯然

超参数科技（深圳）有限公司：

张正生

广联达科技股份有限公司：

宋　楠

广州趣丸网络科技有限公司：

刘亚丹

北京大学：

吴文斐

中国科学技术大学：

徐宏力

# 引言 | Introduction

当前，全球数字化转型进程加速推进，企业作为数字经济建设的关键力量，亟需构建更高效、灵活、安全的数字底座，以支撑多元化业务持续演进。在此背景下，企业网络不再只是基础连接工具，而正演变为构筑核心竞争力的战略资源。云网络作为企业数字基础设施升级的重要方向，正成为支撑业务敏捷部署、算力高效协同与数据快速流动的关键保障。特别是在“东数西算”战略加快实施的驱动下，企业对跨地域算力调用、数据实时传输与异构资源协同的需求持续提升，进一步加速了网络架构向云网融合演进的步伐。

企业数字化进程的加速为云网融合提供了沃土。一方面，企业对跨地域部署、敏捷交付和高可靠互联的需求持续增强，推动云与网络能力的深度整合；另一方面，人工智能、大模型推理、边缘计算等新兴技术的不断涌现对网络提出更高要求，进一步驱动企业网络架构向云原生、智能化、服务化等方向持续演进。

本报告围绕企业级骨干网云化演进趋势展开系统性解析，从发展背景、阶段演进、现实挑战，到云化能力重构、产品设计理念、关键技术支撑，再到安全体系与运维体系的构建，全面梳理“云网融合”在企业场景中的核心价值与发展路径。通过对未来趋势的研判与技术路线的提炼，为企业构建高可靠、高弹性、高智能的下一代骨干网提供参考与启示，以期助力企业在数字化浪潮中把握机遇、构筑优势。

# 目录 | CONTENTS

# 01 企业级云网发展
# 背景概述

# 一 多级政策协同引导，助推企业数字化转型走深向实

在政策引领和战略驱动下，国家正持续加大对企业数字化转型的支持力度，构建协同推进的政策体系和基础保障。

### 政策协同持续发力，全面构建数字化转型支撑体系。

近年来，我国针对“新型基础设施”和“数字经济”重点战略方向进行了密集部署。2023 年 2 月，中共中央、国务院印发《数字中国建设整体布局规划》，指出建设数字中国是数字时代推进中国式现代化的重要引擎，是构筑国家竞争新优势的有力支撑。2023 年 12 月，国家发展改革委、国家数据局等多部门联合印发《关于深入实施“东数西算”工程 加快构建全国一体化算力网的实施意见》，提出整合优化全国算力资源，到 2025 年底初步成型综合算力基础设施体系，推动算力高质量发展。2024 年第二十届三中全会《决定》提出构建新型基础设施规划和标准体系，健全新型基础设施融合利用机制。习近平总书记在 2024 年底召开的中央经济工作会议上指出，数字经济作为新发展动能，具有强大活力与潜力。研究其高质量发展规律导向和趋势变化，有助于我国在全球变革中抓住机遇，应对挑战，提升国际竞争力。2025 年 4 月，国家发改委、国家数据局发布《2025 年数字经济发展工作要点》，提出深入实施数字化转型工程，推进重点行业数字化转型，搭建转型公共服务平台，培育数字化转型服务商。

### 数字基础设施加快建设，网络“大动脉”价值持续凸显。

国家持续从顶层设计、标准建设、产业支持等多方面为企业数字化转型提供全方位支撑，引导企业加快数字基础设施部署、推动数据要素融合与场景创新，构建具有持续竞争力的数字化能力体系。在这一进程中，“东数西算”等重大工程成为典型实践，通过跨地域算力调度优化资源供给、促进数据要素高效流动，并带动多样化应用场景的创新落地。要实现这一系列协同与创新，安全高效的网络环境必不可少，其作为承载与纽带，使“算力调度—数据要素—场景需求”形成闭环。因此，网络不仅是数字基础设施的重要组成部分，更正日益成为构建数字底座和支撑持续创新发展的核心力量。

# 二 市场需求与技术发展交织并进，促建云上数字底座

伴随数字经济的蓬勃发展，企业面临的市场环境日益复杂多变，对云资源的依赖程度不断提升。

### 一方面，企业业务全球化、敏捷化等市场需求促升云基础设施采纳率。

随着全球化业务拓展的深入，企业迫切需要具备全球覆盖能力和高可靠性能的云基础设施，以应对跨地域部署、业务快速响应以及客户服务连续性等挑战。同时，在多元业务场景下，企业对算力敏捷调度、数据快速流转、服务高可用等提出更高要求，推动企业在 IT 系统架构中全面引入云原生理念与实践，特别是在自动驾驶、AI 应用、

车联网、智能家居等 AI 密集型应用场景中，业务需在毫秒级响应中完成推理计算与服务交付，这对网络、算力与存储能力提出极高要求，进一步加速企业对云基础设施的依赖和布局。

**另一方面，企业系统智能化升级布局推动云基础设施价值加速释放。**

人工智能、大数据、边缘计算等新兴技术的快速演进不断重塑企业的数字化能力版图。面对复杂的业务逻辑与海量数据处理需求，企业亟需构建具备高性能、高适应性的智能系统架构，支撑从数据采集、分析、决策到执行的全流程自动化。以人工智能生成内容（AIGC）、语义搜索、个性化推荐等技术为例，企业正在加速集成各类智能能力，实现业务模型的快速演化与迭代。此外，模型与数据分布式部署需求增长，也推动企业从集中式的上云模式，转向以云为核心、边缘协同、端云融合的智能化系统布局，构建可扩展、高韧性、低延迟的新一代业务平台。

**综合来看，云平台正成为数字战略落地的关键依托。**

云平台作为企业数字化运营的主阵地，正逐渐演进为集数据存储、计算、应用托管与服务集成于一体的综合性数字底座。其不仅承载核心业务系统运行，也成为推动组织转型、业务创新的重要依托。可以预见，随着技术与需求的双轮驱动，企业对云基础设施的依赖将持续深化，云将不再只是工具，而成为数字化战略落地的关键载体。

## 三 云网融合拓宽互联边界，构筑企业创新发展竞争力

随着业务云化进程不断深入，企业对网络连接能力提出更高要求，不仅要实现算力与数据的高效协同，还需保障服务的敏捷交付与全程可控。在这一背景下，云网融合加速成为支撑企业高质量转型的新型基础能力。

**云网融合成为打通数据流动与业务交付的关键路径。**

随着企业数字化程度不断加深，传统网络与云平台的分离模式已难以满足高频业务交互和实时数据调度的需求，云网融合应运而生。云网融合通过实现网络与云资源的统一调度与弹性协同，为企业提供更加高效、灵活、安全的数字基础支撑环境。它打破了原有物理边界，实现从“云 - 网分离”向“云网一体”的模式转变，推动资源利用效率大幅提升，助力企业敏捷部署和弹性运维。

**云网融合加快适配多场景需求，提升用户体验与业务连续性。**

云网融合已成为支撑多元化业务场景的关键能力。通过构建“网络即服务（NaaS）”平台，企业能够按需获取网络资源，实现带宽自适应、服务快速上线和安全策略动态调整等功能，大幅提升业务部署效率与服务连续性。同时，借助边缘节点与中心节点协同运行，企业可在靠近用户端实现就近计算与存储，降低延迟，提高体验，对需要高实时性的智能制造、远程医疗、金融交易等场景尤为关键。

**云网融合增强企业网络的安全性与可管理性。**

通过一体化安全策略、全链路加密、行为感知等技术手段，帮助企业实现主动防护和风险预警，有效防范数据泄露与非法入侵。同时，云网融合提升了网络管控的集中性与自动化水平，优化运维效率和系统稳定性。未来，云网融合将持续向智能化、服务化方向演进，成为企业构建可信网络底座、支撑数字化发展的重要抓手。

# 02 企业级云网发展历程分析

# 一 以业务诉求为导向，企业级云网方案分阶段演进

企业级云网方案的演进历程紧随信息技术发展节奏，始终围绕业务效率提升、运营成本控制、安全性保障与可扩展性增强等核心诉求进行演进。其发展大致可分为四个阶段：

### 第一阶段为传统网络阶段（20 世纪 80 年代至 2000 年初）。

该阶段网络以局域网和广域网为主，核心诉求是实现内部资源共享和基础信息传输，网络架构较为简单，强调层次化设计。代表性方案包括 Cisco 推出的 Catalyst 系列交换机，通过支持 TCP/IP 协议，实现企业内网连接。尽管满足了初期办公自动化的基本需求，但缺乏弹性与跨区域互联能力，难以应对多变业务环境。

### 第二阶段为互联网与移动办公兴起阶段（2000 年初至 2010 年左右）。

在互联网普及与移动终端快速发展的背景下，企业级云网对远程接入、安全控制和无线连接提出更高要求。典型方案如 SSL VPN 与无线接入点（AP）部署，使员工可通过公共网络安全访问内部资源，并支持移动办公。然而，该阶段的网络方案依旧以设备部署为主，网络管理与运维复杂度不断上升。

### 第三阶段为云计算与 SDN 融合阶段（2010 年至 2020 年）。

云计算的普及使企业开始重新规划网络结构，SDN 技术的引入带来网络控制与数据转发的解耦，提升了网络资源调度灵活性。代表厂商如华为、VMware（NSX）、Cisco（ACI）等，推出基于 SDN 的数据中心网络方案，实现业务系统快速上线与弹性扩容。尽管网络可编程性大幅提升，但部署复杂性与管理门槛仍较高。

### 第四阶段为智能化与 5G 融合阶段（2020 年至今）。

面向物联网、大模型推理、实时交互等新场景需求，企业级云网需具备更高带宽、更低时延与更强智能。边缘计算、AI 运维、5G 专网等新技术成为主流。华为、Nokia 等厂商推出智能网络管理系统和行业定制化专网方案，具备自我监测、自我修复能力，显著提升了网络适应性与业务连续性。但新兴架构在标准统一性、应用适配性和投资成本等方面仍面临挑战。

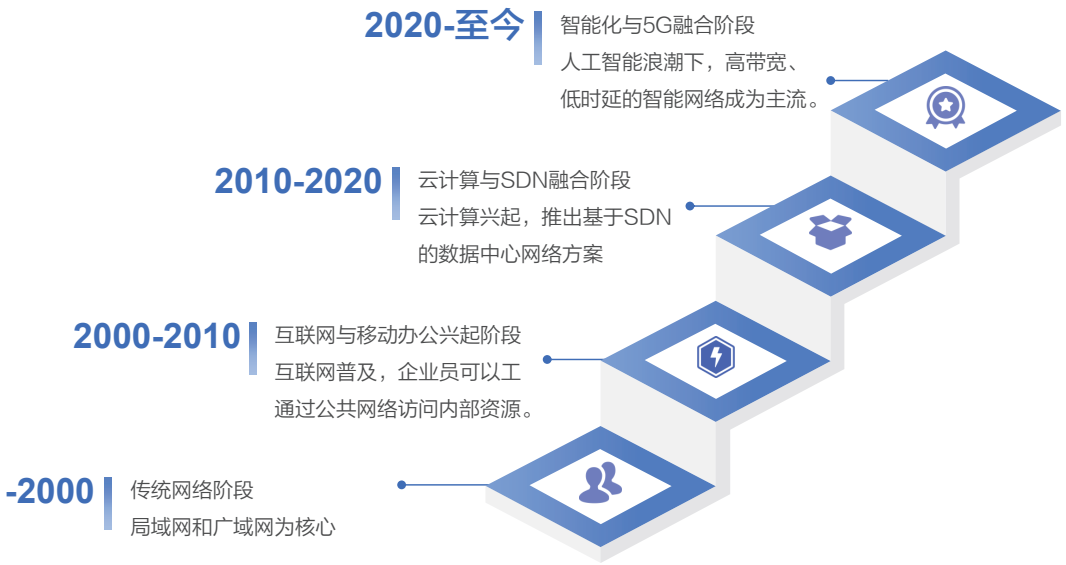



图 1 云网发展历程图

总体来看，企业级云网方案正从静态部署向动态感知演进，从面向设备管理向面向业务服务转型，从中心式架构向分布式云网一体架构迈进。

## 二 以新形势为参照，现有建设方案仍存诸多不足

在云网融合演进过程中，企业网络能力仍面临种种挑战，主要体现在架构适配、性能保障、运维效率、资源利用和安全防护等方面，亟需系统梳理与深入应对。

### 一是架构刚性强，难以适配云化资源动态演进。

传统网络多基于静态拓扑和固定配置构建，缺乏与云资源、分布式架构的协同能力，难以支持弹性扩展、多云接入及异地部署等需求，制约了企业数字基础设施的敏捷性和灵活性。

### 二是性能保障不足，难以支撑关键业务场景。

随着 AI 推理、工业自动化、远程协同等实时性要求不断提升，企业对网络的低时延、高带宽、高可用提出更高标准，而现有架构在网络链路、节点布局、服务编排等方面普遍存在短板，难以保障业务连续性和交付效率。

### 三是管理手段落后，智能化运维水平不高。

网络配置仍以人工操作为主，自动化程度低，缺乏统一视图与智能分析能力，在应对流量激增、链路故障等突发事件时响应不及时，运维压力大，服务稳定性难以保证。

### 四是资源利用低效，带宽成本负担日益突出。

受限于网络资源无法按需调度，企业往往采取冗余预留方式保障业务需求，导致带宽资源利用率偏低、单位成本偏高。尤其在多点部署、跨域访问等场景下，网络传输开销显著，成为制约总体效能的关键因素。

**五是安全防护割裂，全维度风险控制能力不足。**

随着数据跨域流动和访问路径复杂化，企业面临的攻击面持续扩大。但当前网络安全体系多为局部堆叠，策略孤立、设备分散，缺乏端到端的统一安全编排与动态响应机制，难以及时发现风险、形成闭环防护，整体安全韧性不足。

因此，企业亟需构建以业务为中心的新型云网融合体系，系统提升网络的弹性调度、性能保障、智能管理、资源效率与安全防护五大能力，实现云网深度协同，全面支撑未来多元化业务形态与数字生态的持续演进。

## 三 以现代化为目标，企业级云网能力再升级

在企业数字化转型加速、混合云 / 多云架构普及的背景下，企业级云网正从“支撑工具”向“核心竞争力”演进。未来企业骨干网需深度融入云计算基因，以“云网融合”为核心，构建“敏捷、安全、智能、弹性”的新型网络基础设施，成为企业连接多云资源、支撑业务创新的“数字动脉”。

### 1. 一键式创建，全场景覆盖

未来骨干网将基于云原生网络与自动化工具链，实现“场景定义、模板调用、一键部署”的全流程自动化，覆盖企业全业务场景。支持混合云（公有云 + 私有云）、跨地域分支机构、边缘站点接入等典型场景的网络拓扑，支持用户通过图形化界面或 API 调用，快速构建企业骨干网络。

### 2. 多平面隔离，重点应用保障识别

通过云平台的租户隔离技术，比如虚拟拓展局域网（Virtual eXtensible Local Area Network，简称 VXLAN）、多协议标签交换流量工程（MPLS-TE）等技术划分“生产平面”“测试平面”“灾备平面”。各平面独立路由、独立带宽，隔绝业务干扰；针对 P0 级重点应用（如实时交易），预留专用带宽，结合 QoS 策略实现端到端低时延、零丢包的保障；对 P3 级普通业务（如文件备份），基于负载情况动态调整带宽，避免资源浪费。

### 3. 智能管控中心统一调度，流量全局可视

未来骨干网将依托云化管控平台 +AI 算法，构建“可观测、可预测、可优化”的智能管控体系，实现流量的“全局可视、精准调度”。基于云原生微服务架构，骨干网控制器集成流量采集、分析、决策功能，与云平台监控（如 Prometheus）、日志（如 ELK）系统打通，实现“网络 + 云 + 应用”全链路数据融合。

### 4. 弹性资源按需取用，闲忙时段差异化计费

骨干网采用“软件定义”架构，网络带宽、转发节点等资源通过虚拟化技术整合为资源池，支持秒级扩缩容（如

根据实时流量自动增加 10Gbps 带宽）。结合历史流量数据（如工作日 9:00-18:00 为忙时，23:00-6:00 为闲时），骨干网控制器自动调整资源分配：

忙时：优先保障核心业务，动态调用备用链路或云化资源；

闲时：释放冗余资源，降低设备功耗；或启动数据传输备份等非实时业务。

### 5. 分权管控，零信任接入，敏感业务加密

未来骨干网将构建“分权管控 + 零信任接入 + 端到端加密”的多层安全体系，实现“最小权限、持续验证、全程加密”。融合云计算 Landing Zone 解决方案基于角色的访问控制（RBAC），为不同部门分配差异化权限，避免“越权操作”。集成多因素认证、设备健康检查，仅允许“可信设备 + 可信用户”接入；对敏感业务采用加密算法及加密协议，实现端到端加密。降低数据泄漏风险，减少误操作导致的故障率。

# 03 企业级骨干网络云化设计理念与技术方案

在企业数字化转型不断深化的过程中，业务对算力、数据和应用的依赖日益增强，分布式部署与多场景协同已成为常态。然而，单点式、局部化的网络已难以满足跨区域、跨平台和跨终端的高效协同需求。为此，企业需要构建统一、稳定、智能的骨干网络，作为承载和联通的关键枢纽。同时，企业级骨干网络的设计应兼顾一体化布局、智能化调度与安全可控，既要突破传统边界，又要为全局业务提供高效、稳定与可信的支撑，为企业构建敏捷、智能、可持续演进的数字化网络环境。

## 一　核心理念：打破边界，构建“云 - 边 - 端 - 办公”一体化网络

未来企业级云网应以“全局一张网”重新定义企业网络边界，通过云原生架构与统一管控平台，将分散的云资源、边缘节点、办公终端、分支网络整合为逻辑一致的“虚拟网络”，实现“任意节点、任意业务、任意场景”的无缝互联。

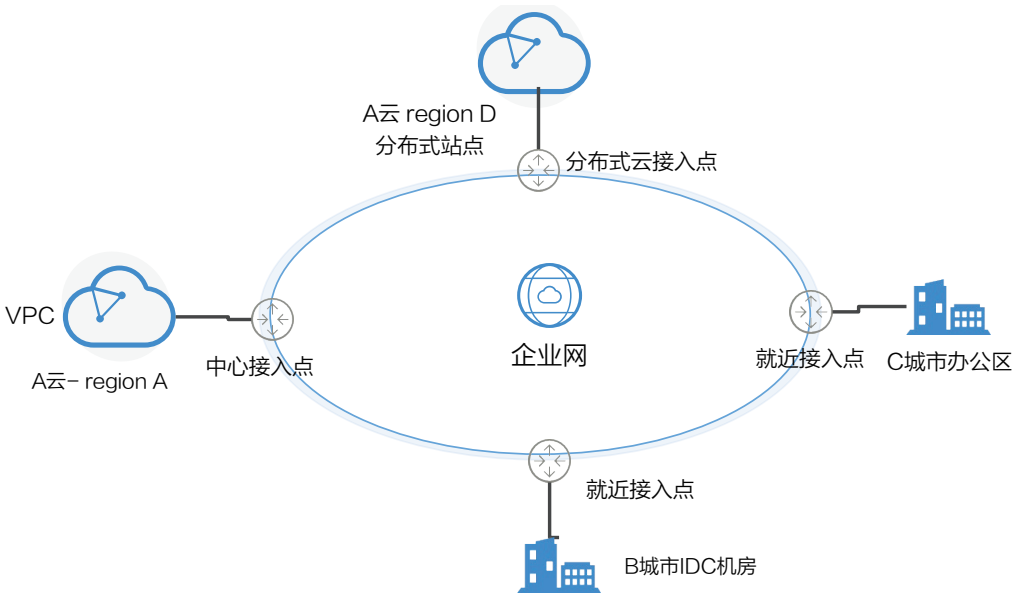



图 2 企业级云网串联企业分散的资源站点

基于云基础设施平台能力，构筑云化的企业骨干网，为企业级互联、调度、管控提供了便利性。依托于多家运营商的冗余和无缝切换，实现 99.99%+ 的可靠性组网架构。

## 二　企业级互联：构建全场景智能互联基础

企业级骨干网是支撑企业数字化转型和业务创新的核心基础设施，是连接企业总部、分支机构、数据中心

和云资源的关键传输通道。骨干网云化后带来核心的关键特征：

### 1. 一键式互通，全场景覆盖。

基于云骨干网基础设施架构的协同能力，实现弹性组网，零配置自动化，提高了基础设施的敏捷性和灵活性。

云厂商将骨干网接入设备部署到客户就近的入网点（PoP 点），方便客户便捷接入；PoP 点覆盖国内各个大区，甚至海外重点城市，给企业接入提供了极大便利。

对比传统组网方式，云化骨干网具有以下优势：

**提供业界标准的界面与 OpenAPI，支撑零配置一键创建。**

**提供网络可视化界面和监控界面，全局视角网络管理与监控。**

**提供云化后带宽弹性能力，识别流量大小自动调整线路带宽。**

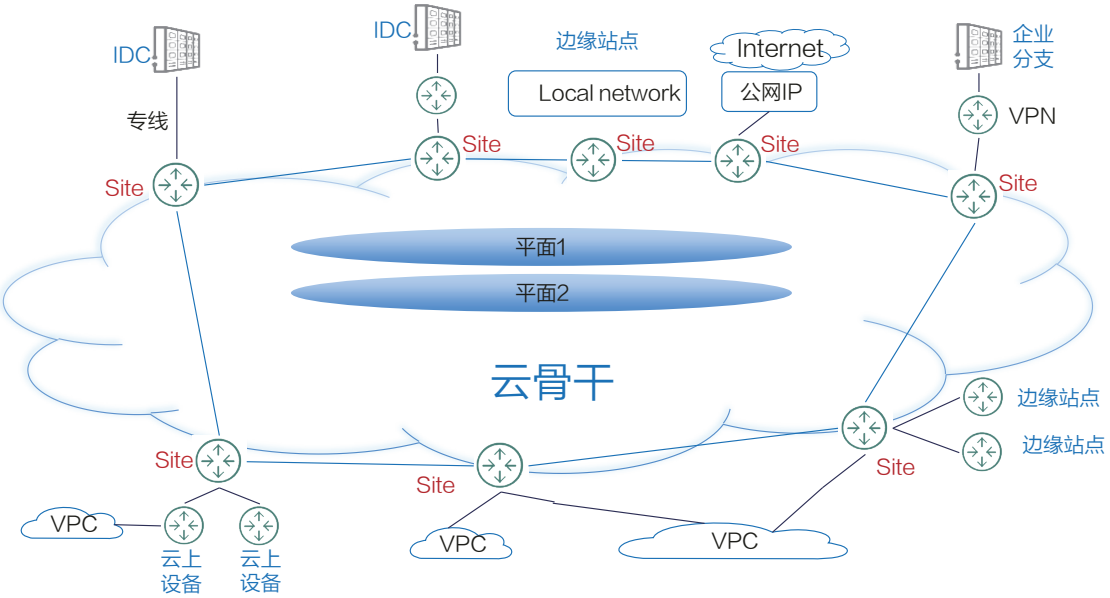



图 3 云骨干网示意图

### 2. 就近接入，无缝整合。

如上图所示，企业云网络可以将连接企业总部、分支机构等多地数据中心网络和云上中心 VPC、云边缘站点 VPC 等多场景网络接入到企业级云骨干网，实现全地域、全场景的网络覆盖。

云化骨干网可以支持客户丰富的各种场景的接入方式：

**企业总部接入：**支持客户侧 SD-WAN 设备接入，配套一站式专线。

**企业站点接入：**客户侧 VPN 设备接入。

**终端接入：**VA 零信任接入，5G 备份接入。

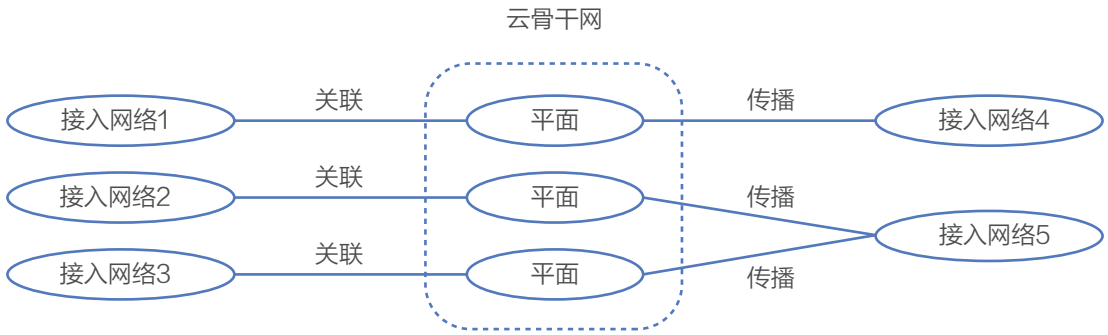
**云网络接入：**无缝接入 VPC 等云上网络。

企业级云骨干网深度融合总部、分支、终端与多云场景，提供 SD-WAN 专线、5G 备份、VPN 零信任及 VPC 无缝接入，以智能网络架构实现全地域、全场景的敏捷互联与统一管控，赋能企业数字化转型。

### 3. 多平面隔离，重点应用保障识别。

企业级云网支持多业务平面的隔离，以确保不同业务之间的数据安全和性能独立。例如根据业务类型（生产业务、测试业务、视频会议）划分不同的业务平面，每个平面独立运行。通过路由表隔离（VRF）、虚拟拓展局域网（VXLAN）、虚拟私有网络（VPN）等技术，确保不同业务平面之间的数据传输安全，避免业务干扰和数据泄露。

为了达到多平面的效果，企业云骨干网通过定义“关联”和“传播”来描述平面与接入网络的转发关系，接入网络通过“关联”定义流入企业级云骨干网的平面，通过“传播”来定义流出企业级云骨干网的平面后所到达的目标接入网络。“关联”关系中平面与接入网络必须是一比一。“传播”关系中接入网络与平面可以是一比多。




注：网络1流量可以流向网络4，无法流向网络5；网络2、网络3流量可以流向网络5，无法流向网络4

图 4 云骨干网关联和传播示意图

企业级云骨干网兼顾企业业务的灵活性、安全性和扩展性。通过支持多业务平面隔离、安全互通、灵活接入等特性，企业级云网可以满足企业在数字化转型中的多样化需求。企业级云骨干网领域的技术，企业可以进一步提升网络的智能化、自动化水平，构建高效、安全、可靠的网络基础设施。

## 三 企业级调度：实现关键业务精准保障能力

云骨干网络技术分为物理层和业务层。其中物理层，管理着大量的物理线路和设备，形成拥有海量互联资源的网络资源池；业务层，提供给企业客户抽象的云骨干网服务能力，即 API 化即开即用的骨干网服务。因此企业客户无需关注物理层的链路和设备管理，以及资源调度，仅需要根据配置对应的逻辑路由器、路由表、逻辑通道实现网络互联，以及对应网络 QoS 和 SLA 诉求即可，云骨干网关技术架构，需要将相应的诉求，将客户的流量，调度到对应的物理链路上，并能根据网络的拥塞、丢包、故障等状态，实时调整流量使用的链路，保证企业客户

业务流量的 SLA。

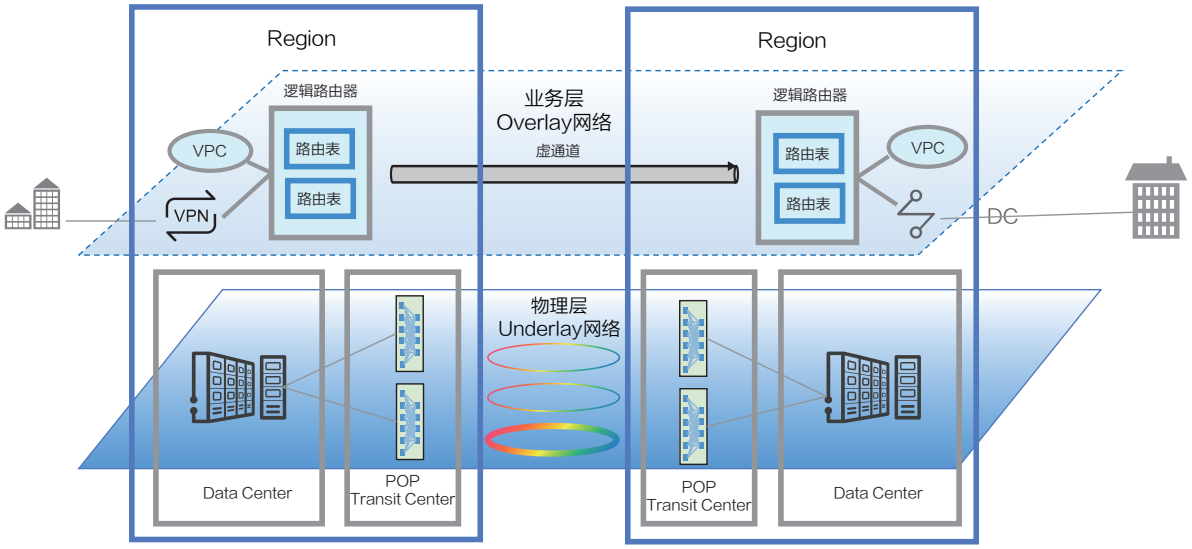



图 5 云骨干网物理层和业务层示意图

## 1. 云骨干网络 SLA 及 QoS 功能定义

企业使用云骨干网的过程中，由于其业务多样化的诉求，对云骨干网的 SLA 和 QoS 都会有不同的诉求，例如音视频业务，需要低时延及低丢包率，而一些定期备份类业务，则需要大带宽，对时延不敏感。首先是涉及到对于网络带宽的诉求，不同的网络平面对应不同的虚通道，每个虚通道都可以设置单独的带宽诉求，而且可以基于物理网络资源池，实现虚通道带宽的按需使用；其次涉及到对网络 SLA 的诉求，可以为虚通道或者虚通道内部的不同类型业务，设置不同的服务等级，并定义不同等级下的时延、丢包率等指标。最后是灵活的计费策略，方便企业客户根据各自业务特点，实现根据质量的差异化计费，或者根据时段的差异化计费，促进对于网络带宽的充分使用。

### 虚通道的带宽诉求

**带宽保障：**企业客户可以指定虚通道的最低带宽，在任何情况下，云骨干网需要保障客户可以使用到指定的带宽

**带宽峰值：**企业客户为避免过度使用带宽，导致企业使用骨干网的费用超支，企业客户可以为虚通道指定带宽峰值，云骨干服务网需要实现带宽的限速能力

**业务优先级：**虚通道内的业务流量达到带宽峰值的时候，需要能够保障根据业务优先级丢弃报文，保证高优先级的业务优先使用带宽。企业客户可以通过策略（IP 地址、端口等）或者应用特征（基于 DPI 深度感知）指定业务的优先级。

### 业务的 SLA 诉求

**基于虚通道的 SLA 诉求:** 客户能够按照自身业务的重要性和敏感性，提出对网络性能的具体要求，如丢包率、时延等关键指标。为满足差异化需求，网络可提供金、银、铜多级 SLA 服务等级，并在各等级中明确规定不同的丢包率、网络时延等性能标准。

**基于业务的 SLA 诉求:** 在虚通道内，企业客户可以通过策略规则（如 IP 地址、端口等）或应用特征识别（基于 DPI 深度感知）来指定对丢包率、网络时延等关键指标的要求。为满足不同业务场景，网络可提供金、银、铜多层级的 SLA 服务等级，并在各等级中明确对应的性能标准。

### 云骨干网计费诉求

**基于流量的计费：**根据企业客户实际使用的流量计费，计费时，需要考虑云骨干网的距离和 SLA 质量，实现差异化计费 。

**基于带宽的计费：**根据企业客户固定的带宽包计费，或者根据客户实际使用的带宽计费，包含 95 计费策略等。计费时，同样需要考虑云骨干网的距离和 SLA 质量，实现差异化计费。

**基于时段的计费：**根据忙时和闲时制定差异化计费策略，方便企业客户在闲时使用骨干网做海量数据备份等非实时的业务。

## 2. 云骨干网调度组件及功能要求

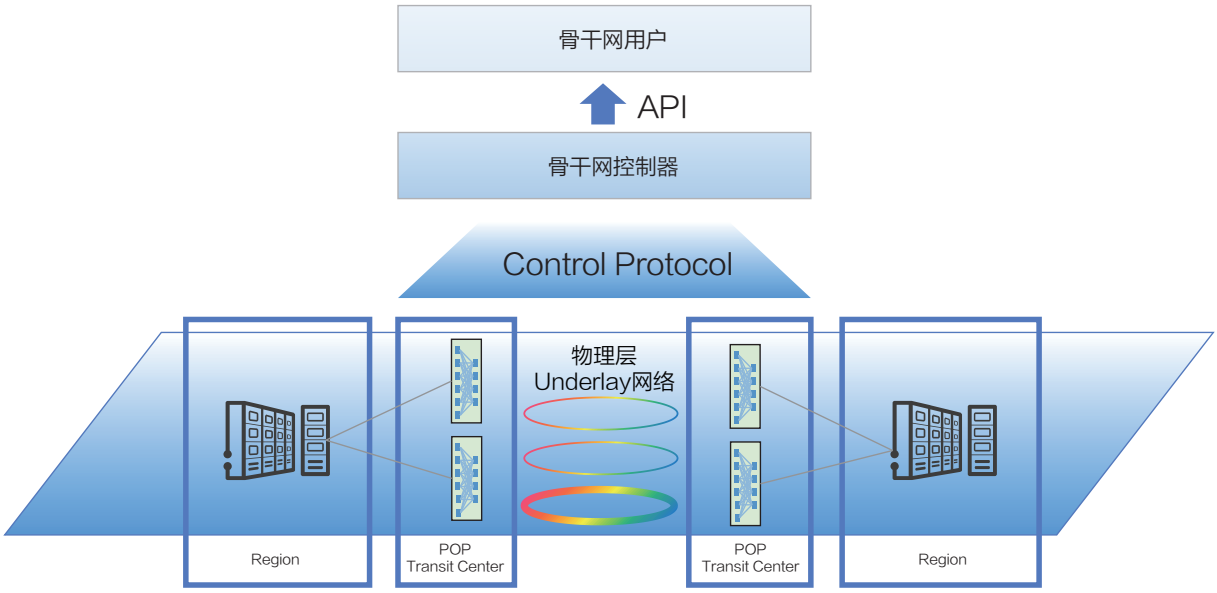



图 6 云骨干网调度示意图

### 云骨干网物理设备

云骨干网物理设备，主要包括 PoP/Transit Center 中的相关设备，这些设备需要支持源路由能力，例如基于 MPLS 标签的源路由能力或 SRv6 的源路由能力，便于针对不同的业务进行选路。同时要支持网络链路的使用状态采集能力，包括各个链路的带宽使用量，网络接口的丢包统计，骨干网相邻节点的时延检测，也要支持隧道级别的丢包、时延统计，支持基于隧道粒度的带宽上下线设置能力。

### 云骨干网控制协议

云骨干网物理设备需要支持云骨干网控制协议，以便能够将网络状态上报给云骨干网控制器，同时能够接受控制器的指令，建立相关的转发隧道，可以使用准协议，也可以使用自研的 API 协议和控制器互通。通过骨干网控制协议，网络设备可以上报收集拓扑（BGP-LS），收集流量信息，收集链路质量状态、收集隧道路径信息，然后下发 MPLS 标签路径，或者 SRv6 SRH 显式路径。

### 云骨干网控制器

云骨干网控制器是整个骨干网的大脑，管理整个骨干网的链路状态，并提供北向接口向高阶使用者提供服务。

云骨干网控制器北向接口，定义了高阶业务的网络诉求接口，高阶业务在使用骨干网的时候，需要向骨干网控制器说明业务所需目的地信息、带宽需求（带宽上下限）、SLA 需求（丢包率、时延等）、使用时段等诉求，也包括业务使用带宽的时间需求。同时，为了让网络设备识别对应的业务报文，并将报文引入到即将建立的隧道中，高阶业务模块需要通过北向接口和骨干网控制器协商业务报文识别方式，因此业务模块会给出建议的业务流量特征，比如源目的 IP 地址，DSCP 等信息，这些信息用于骨干网控制选择具体的报文识别方式。

云骨干网控制器根据上述北向接口业务诉求，并根据从云骨干网控制协议获取到网络链路状态，计算出合适的网络路径，生成隧道及其转发表项，并将转发表项下发到网络设备。同时，为了让网络设备也会明确识别业务报文的方式，例如源目的 IP 地址或 DSCP 信息，通过北向接口返回给高阶业务

## 3. 骨干网调度策略要求

云骨干网控制器管理着大量的骨干网设备和通信链路，这些通信链路可以有不同的来源，有不同的成本，以及不同的可靠性质量。骨干网控制器需要通过北向接口对高阶业务提供骨干网服务，每一次高阶业务通过 API 请求骨干网资源时，骨干网控制器都需要根据业务的诉求，计算网络路径并生成隧道。计算网络路径的过程，需要考虑如下策略：

**成本最优策略：**在满足带宽以及 SLA 要求的情况下，选用成本较低的链路，降低客户的使用成本。

**可靠性最优策略：**根据客户 SLA 以及业务特征，找到最合适的网络链路，例如高 SLA 要求的音视频业务，

优选高质量链路传输。

**时间段最优策略：**根据网络链路的忙闲时段的统计与预测，给出使用的时间段建议，保证整个网络在所有的时间段都能够均衡地被使用，削峰填谷，避免业务高峰期的拥塞。

# 四 企业级管控：构建主动安全纵深防御体系

企业云骨干网的管控体系需以“全局视角、动态信任、全链路防护”为核心，通过与云 Landing Zone 深度整合，构建“统一管控中心 + 账号分权治理 + 端点零信任接入 + 链路端到端加密”的立体安全架构，实现从“被动防御”到“主动智防”的跨越。

## 1. 统一管控中心：云网全局指挥中枢

传统网络安全的痛点在于“分散管理”——网络设备（路由器、防火墙）、云平台（公有云、私有云）、安全工具（SIEM、IAM）各自为政，导致威胁响应滞后、运维效率低下。云骨干网的统一管控中心通过“云化架构 + 开放接口 + 智能引擎”，打破多系统壁垒，实现安全能力的集中调度与全局可视。

统一管控中心基于云原生微服务架构构建，通过标准 API 与云平台、网络设备、安全组件深度集成，形成“统一入口、统一策略、统一监控”的安全中台。在这一架构支撑下，管控中心具备三方面核心能力：

**集中管理：**通过云平台的软件管理能力，统一对接云骨干网中的每一个网络设备，一键式配置实现端到端打通；集中管理骨干网中安全控制节点，如云防火墙（CFW）、网络访问控制（ACL）、接入点安全认证方式等，实现全网的集中控制统一调度。

**统一呈现：**整合全网流量日志、设备状态、云资源日志等，通过 AI 算法（如异常检测、威胁图谱）实时识别潜在风险。

**一键调度：**针对现网的异常流量和特殊业务场景，一键式溯源识别，源端反压等，消除现网风险，减少人工干预。

## 2. 云网 landing zone：账号分权管控及组织边界安全

Landing Zone 是企业上云的“安全合规基线”，通过企业骨干网深度整合，可实现“角色 - 权限 - 资源”的精细化匹配，避免“越权操作”“权限泛化”等安全风险。通过 Landing Zone，可以实现云骨干网的预防性安全策略以及检测性安全策略，预防性安全策略着眼于源头防控，遵循“预防胜于治疗”的原则，通过主动设计降低威胁发生的可能性，在问题暴露前即消除隐患，例如阻断未授权账户对云骨干网的恶意操作与配置。检测性安全策略则聚焦于事中监测与快速响应，通过实时监控与告警机制识别已发生的风险事件，缩短处置时间，降低

损失风险，对管理员的错误配置进行及时发现与告警。

在此策略框架下，Landing Zone 进一步通过三方面机制实现精细化安全管理：

**角色定义（RBAC）：**根据企业组织架构（如 IT 运维、业务部门、审计）与业务需求（如生产、测试、灾备），定义差异化角色（如“网络管理员”“安全审计员”“业务访问员”），每个角色绑定“最小必要权限”（如仅能查看日志、配置策略、访问特定业务）。

**动态权限校验：**结合时间（如仅工作日 9:00-18:00 生效）、位置（如仅允许企业办公网访问）、设备（如仅安装指定杀毒软件的终端）等条件，动态调整用户权限（如财务人员夜间无法访问核心数据库）。完善所有账号和资源的 SCP、NCP、RCP 权限。

**账号分权制衡：**网络管理员、安全管理员、审计员等账号相互校验。网络管理员可配置网络路由连通及平面隔离策略，安全管理员可配置安全管控策略，基于接入点的安全合规性审批接入权限；而审计员可做三方合法合规性 check，减少人员权限过大或人因差错导致的配置漏洞

## 3. 骨干安全：零信任接入与端到端加密

传统 VPN 或防火墙依赖“IP 地址 + 固定权限”的静态认证模式，无法应对“远程办公、移动设备、第三方协作”等场景下的动态访问需求。云骨干网的零信任安全接入体系通过“持续验证、最小授权、动态加密”，构建“端 - 管 - 云”一体化的可信访问通道。该体系主要通过以下两个环节实现：

**站点接入认证：**某一个 site 站点建立骨干网链接，需进行安全密钥协商和认证。接入前检测路由设备的安全状态（版本补丁合规、密钥凭证合法、是否存在恶意进程），仅允许“健康设备和健康站点”接入。

**用户接入认证：**用户登录时需通过“密码 + 动态令牌 + 生物特征（指纹 / 人脸）”三重验证，防止账号盗用；结合用户身份、访问时间、设备位置、请求的资源类型（如生产数据库 / 测试 API）等上下文信息，动态评估风险等级并授予最小权限（如仅允许读取数据，禁止删除）；客户的零信任接入能力，也包括客户运行环境的检查，包括运行的操作系统及补丁、安全软件及版本、本地是否有涉密信息等。同时骨干网的零信任接入网关，需要支持基于上述信息的 ABCA 安全策略配置，即通过策略文本，控制客户可以访问的网络、应用，以及对应用、数据的访问权限。

在零信任安全接入体系确保“谁能进来”的基础上，数据安全则进一步聚焦于“进来之后如何保护”。作为企业的核心诉求，云骨干网通过端到端加密能力覆盖“传输 - 存储 - 处理”全链路，确保敏感数据实现“偷不走、解密难、用不了”。围绕这一目标，云骨干网的数据安全机制主要体现在三个方面：

**KMS 中央派发密钥：**通过云服务 KMS 密钥派生，再进行统一加密推送密钥，实现多个 site router 之间免协商 fullmesh 互联，既解决了多点密钥协商的困境，也完美实现集群加密能力解决性能问题；同时，基于 KMS 管

理密钥，定期轮转，避免长期使用同一密钥导致的安全风险。

**自定义加密算法：**基于云平台自研 site router 设备，自定义云平台加密算法；通过自研 router 加密模块，开发仅本平台才识别的加密协议，大大加强了加密算法的安全性。

**应用层加密：**所有接入流量通过 TLS 1.3 或国密 SM4 算法加密，防止中间人攻击（MITM），敏感业务（如金融交易）额外启用双向证书认证，满足《中华人民共和国网络安全法》《中华人民共和国数据安全法》的相关规定。

# 五 企业级可靠性：打造毫秒级韧性网络底座

在数字化转型的核心场景中，企业业务连续性直接依赖于骨干网络的抗风险能力。传统单链路依赖的架构已被淘汰，云网融合时代的骨干网需通过多维度可靠性设计，将底层物理容灾与智能运维可视化深度绑定，构建真正的企业级韧性网络。

## 1. 多运营商智能调度：从物理冗余到服务级带宽

**运营商异构链路池化：**云骨干网融合移动、电信、联通、国际运营商以及云厂商自建线路的多路径物理链路，通过边界网关协议（BGP）与任播（Anycast）+ 软件定义网络（SDN）动态选路技术，实现跨运营商的毫秒级智能切换。

**SLA 驱动的流量调度：**云骨干网根据实时网络状态（延迟、丢包率、抖动）及业务服务品质协议（SLA）需求（如视频会议 <50ms，数据同步 <1% 丢包），适配优先级等价多路径路由（WCMP）算法，自动分配最优运营商路径。

**带宽成本优化：**云骨干网基于线路池化与智能流量调度，支持按需调用低价冗余链路，在保障关键业务可靠性的同时降低线路成本 30% 以上。

## 2. 云原生高可靠：从硬件容错到协议层自愈

### 物理层：坚实基座

云骨干网实现全设备冗余，涵盖设备内部关键部件（如主控板卡、电源模块、采用 N+1 配置的风扇等），确保核心功能在局部故障时无缝接管；在网络架构层面，接入层、汇聚层、核心层均部署多重冗余机制采用堆叠/M-LAG，快速重路由（FRR）等技术，构建真正意义上无单点故障的物理架构，为上层业务提供坚实的硬件基石，有效避免设备级宕机引发的业务中断。

### 协议层：毫秒自愈

云骨干网通过多种协议协同构建底层网络（Underlay）与客户网络（Overlay）的快速自愈机制，形成端到端的高可靠保障体系。

在 Underlay 层面，部署高效的协议闭环以确保网络的稳定性与快速恢复能力：

**链路聚合控制协议（LACP）：**提供接入层链路毫秒级冗余切换与负载均衡；

**边界网关协议（BGP）：**实现稳定路由控制和拓扑快速收敛，应对节点或链路故障；

**双向转发检测（BFD）：**提供毫秒级精准的连通性检测，为倒换协议提供实时故障信号。

在 Overlay 层面，通过软件定义网络（SDN）驱动的智能探测机制并基于集中控制与虚拟化隧道技术，构建与物理网络解耦的逻辑自愈体系，通过动态路径重构与策略化流量调度实现业务无感知故障恢复。其核心协议与技术包括：

**冗余隧道：**结合底层网络的多等价路径路由（ECMP），建立多条物理链路承载的 Overlay 逻辑隧道，单隧道故障时流量自动切换至备用隧道（切换时延≤ 50ms），业务零中断迁移：支持虚拟机 / 容器跨数据中心热迁移，IP 地址与策略随动，保障会话连续性；

**增强型 BFD for Overlay：**针对 OverlayLay 隧道部署毫秒级探测（检测间隔≤ 10ms），实时感知虚拟路径故障。

通过 Underlay 与 Overlay 的协议无缝协同，云骨干网构建了快速感知 - 精准诊断 - 即时切换的闭环自愈机制，将网络层故障收敛时间严格控制在亚秒级（典型值 <200ms），从而为企业业务连续性提供有力保障。

### 应用层：智能避障

云骨干网引入基于大数据与人工智能（AI）的流量预测引擎，持续学习历史与实时网络状态，精准预判未来潜在拥塞风险；并联动智能调度系统，依据预测结果主动执行最优路径选择、负载均衡优化及策略路由调整（依托 SDN 控制器或 Telemetry 技术），实现“预测 - 分析 - 决策 - 执行”的闭环管控，在拥塞发生前将流量智能调度至最优或空闲链路。这从应用层面主动规避了性能瓶颈，显著提升了用户体验稳定性和整体链路资源利用率。

## 3. 运维可视化：全维度态势感知与智能决策中枢

运维可视化是企业骨干网的“数字神经中枢”，通过多源数据融合与 AI 分析，实现物理层至应用层的全栈可观测性，支撑故障秒级定位与资源动态调优。

### 逻辑拓扑图

自动绘制 Overlay 网络路径，标识 SDN 控制器调度路径与协议层自愈状态（如 BGP 收敛耗时、BFD 检测频次）

### CES 云监控（全栈指标采集）

云服务监控：实时检测云资源状态（如网关流入流量、流出带宽、骨干线路丢包时延），图标颜色动态标识异常（灰→红），支持仪表盘 / 数字图等多图表切换。

### 流日志（网络层行为分析）

五元组深度解析：追踪源 IP、目的 IP、端口、协议、流量动作（允许 / 拒绝），识别异常流量模式（如 DDoS 攻击源、跨区违规访问）

智能诊断建议：基于历史基线比对，自动推送优化策略（如“安全组规则阻断合法流量，建议放通端口 XX”）

### CLS 日志审计（安全与合规管控）

关联分析引擎：聚合设备日志、操作审计、入侵检测数据，生成攻击链图谱（如“异常登录→敏感文件下载→外联 C2 服务器”）

合规基线库：预置等保 2.0/ISO27001 策略模板，自动检测配置偏离并生成整改报告

### 工单自动化闭环

可视化 SOP：故障处理流程嵌入拓扑图，自动分配责任人并推送处置指引（如“数据库主备切换操作手册”）

# 04 场景实践

# 一 某游戏 AI 领域企业通过云骨干网实现全球网络智能调度

## 1. 案例背景

A 企业是一家专注于 AI 与游戏深度融合的创新型科技公司，致力于为全球游戏开发者提供先进的游戏 AI 解决方案。其开发的游戏 AI 智能体具备高度自主决策能力和深入的环境交互能力，在全球范围内率先实现了 Game Agent 技术的大规模商业化落地，目前已服务了腾讯、米哈游、莉莉丝、西山居等众多行业头部企业。相关产品已在多款日活超千万的头部产品中得到应用，覆盖全球 65 个国家与地区，并保持着长期、高效、稳定的运行表现。

### 网络性能要求：

游戏服务器发送调用 AI 机器人请求到收到响应，端到端时延要求小于 200ms，超时比例小于 0.05%；游戏服务器连接丢包率小于 0.001%。

### 核心目标：

在全球范围内，为游戏厂商提供高可靠、低延迟的 AI 机器人服务，实现云端调用的极致性能，确保玩家体验流畅。

## 2. 架构痛点

### （1）网络架构可扩展性与可靠性问题

**低缺乏统一的全球化网络架构：**

游戏厂商的全球化部署需求导致跨国网络环境复杂，传统网络架构无法灵活适配游戏服务器与 AI 机器人之间的动态流量需求，存在以下问题：

**多供应商与异构网络：**各区域网络解决方案不统一，互通性差，网络拓扑复杂。

**冗余设计不足：**跨数据中心与跨区域的链路缺乏合理的冗余设计与故障切换机制，一旦发生故障可能影响玩家游戏体验。

**高峰流量带来的网络瓶颈：**

游戏高峰时段，玩家访问量激增，导致调用 AI 机器人的请求拥堵，无法保障时延和丢包率的要求。

**未来扩展性不足：**

当前网络架构难以匹配未来游戏厂商对 AI 服务的更高需求，如边缘计算、实时音视频互动、AI 生成内容（AIGC）

等新兴技术的接入。

### （2）网络调度能力不足

**静态路由与固定链路：**

使用传统固定链路和静态路由设计，游戏服务器到 AI 服务器之间无法根据实时负载、链路质量动态调整路径，导致部分链路拥堵而其他链路资源闲置。

**缺乏智能流量调度：**

无法根据业务优先级（如关键游戏场景的 NPC 响应、多人联机对战的实时指令）动态调整流量路径，导致时延和丢包率不符合 SLA。

**跨区域协同困难：**

游戏服务器部署在全球不同数据中心，AI 机器人服务需要支持全球玩家的就近接入，但由于缺乏智能调度，难以实现最优路径选择。

### （3）线路部署周期长，运维复杂

**新增业务上线慢：**

游戏厂商上线新游戏或新功能时，需要重新配置网络链路，流程复杂且耗时长，无法满足快速上线需求。

**运维效率低：**

网络配置与策略调整依赖手动操作，容易出错且效率低下。排障时无法快 速定位问题区域，影响玩家体验。

## 3. 解决方案

A 企业基于云网融合架构，构建低延迟、高可靠的全球 AI 机器人服务网络，通过智能调度与自动化运维能力，确保游戏厂商在全球范围内的业务连续性和用户体验。

### （1）云网融合的全球化网络架构

**覆盖全球的接入与覆盖网络：**

基于 A 企业的全球分布式接入点（如 POP 点、边缘节点、云入口网关），通过云公网、云专线、全球加速、VPN 接入等多种方式，为游戏厂商提供“一跳入云，全球通达”的网络服务：

用户（游戏服务器）根据地理位置与网络质量，自动选择最近的接入点。

专线传输提升带宽与稳定性，保障关键游戏场景的低延迟需求。

**弹性扩展与智能调度：**

通过软件定义网络（SDN）与网络功能虚拟化（NFV）技术，构建动态、灵活的网络架构：

网络资源（如带宽、IP、链路）按需分配，适应游戏高峰流量。

自动化部署能力支持新游戏、新区域快速接入，缩短上线周期。

### （2）智能流量调度与优化

**实时流量感知与智能调度：**

基于云平台的网络监控中心，实时感知链路状态、流量负载、延迟等关键指标，自动选择最优路径：

应用级流量调度：优先保障关键业务（如多人联机、支付交易）。

动态链路选择：根据链路质量、负载情况实时调整路径，避免拥堵。

**多路径传输与负载均衡：**

采用 ECMP（Equal-Cost Multi-Path）、Anycast 等技术，实现多路径并发传输，提升网络可靠性与冗余性。

### （3）安全增强与访问控制

**零信任接入模型：**

基于用户身份、设备状态、访问上下文动态调整访问权限，防范内部威胁与数据泄露。

**分布式安全防护：**

集成 DDoS 防护、流量清洗、入侵检测等功能，实时应对网络威胁，保障游戏厂商业务安全。

### （4）自动化运维与监控

**自动化配置与编排：**

云平台支持网络策略的集中化管理与自动化部署，将网络配置时间从“天 / 周”级缩短到“分钟 / 秒”级。

**异常检测与快速恢复：**

系统能够实时分析流量异常并触发自动化调度策略，如故障切换、流量清洗等，保障业务连续性。

## 4. 收益效果

**保障业务高峰稳定性：**

网络架构支持弹性扩展与按需分配，确保游戏高峰期不卡顿，低谷期不浪费。

**降低时延与丢包率：**

优化的接入路径与智能调度，确保端到端延迟 <200ms，丢包率 <0.001%，显著提升玩家体验。

**提升运维效率与敏捷性：**

自动化运维将新游戏上线时间缩短至分钟级，降低人工干预风险。

**增强安全性与合规性：**

零信任架构与分布式防护机制提升网络安全水平，满足数据隐私与行业合规要求。

**支持全球化与未来扩展：**

可扩展的云网络平台无缝连接游戏厂商的本地数据中心、全球云节点与边缘设备，为未来技术创新提供坚实基础。

**提升用户体验与满意度：**

高可靠、低延迟的网络服务，让玩家在全球范围内享受一致的游戏体验，增强厂商品牌竞争力与用户黏性。

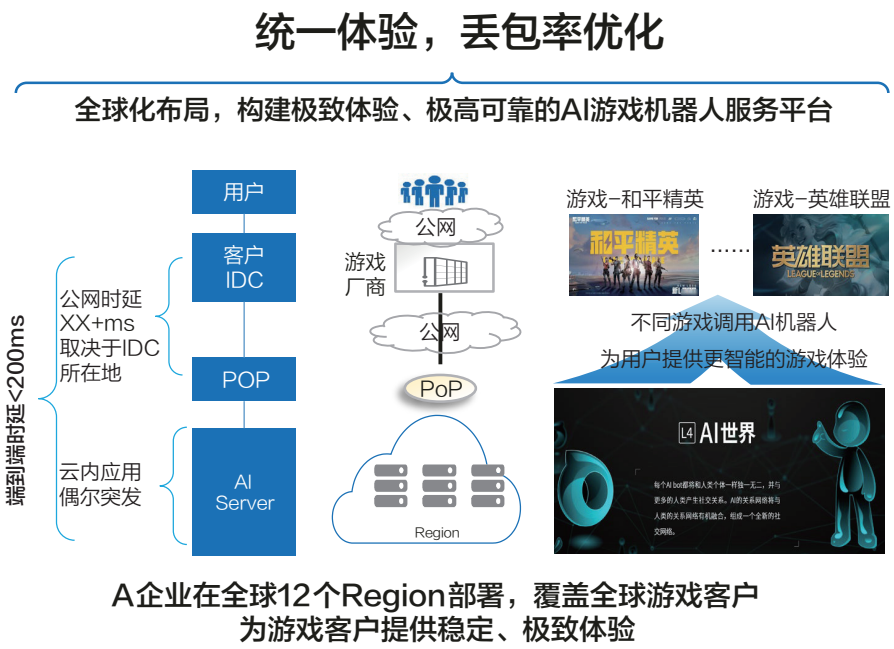



图 7 A 企业优化后组网图

通过以上解决方案，A 企业为游戏厂商提供了覆盖全球、低延迟、高可靠的 AI 机器人服务，助力构建“10 亿人与 100 亿 AI 共同生活的虚拟世界”。

# 二 某传统企业通过云骨干网构建高可用网络

## 1. 案例背景

B 企业作为中国领先的数字建筑平台服务提供商，在数字化转型的过程中，逐步向云端架构演进，以满足业务快速增长与灵活部署的需求。B 企业的业务覆盖全国，服务包括建筑施工、成本管理、项目管理等多个领域，其 IT 架构需要支持多云混合部署和高可用需求。

为解决传统网络架构的可用性与灵活性不足的问题，B 企业通过环形拓扑、BGP 动态路由等技术，构建了高可用的混合云网络，显著提升了业务连续性与网络运维效率。

## 2. 业务痛点

B 企业在传统架构中仅采用单链路连接各节点，一旦链路发生故障便会直接导致业务中断，整体可用性较低；同时，静态路由依赖人工手动配置，过程繁琐且缺乏动态学习能力，在路由调整时需人工介入，存在较高的出错风险；此外，各 VPC 之间均通过对等连接实现互联，形成复杂的网状拓扑结构，每当新增或调整 VPC 时均需修改大量配置，导致运维维护成本高昂。

## 3. 解决方案

为构建高可靠、智能化的云互联网络，B 企业采用环形冗余链路与 BGP 动态路由相结合的整体架构，并依托华为云骨干网实现统一高效的全网互联。具体实施方案如下：

首先，通过新增北京二期至华为云的专用链路，构建环形拓扑结构，形成链路级冗余，彻底消除单点故障，显著提升物理链路的可靠性。

其次，将各虚拟私有云 VPC、专线网关 DC 统一接入华为云骨干网，构建简洁高效、易于扩展的云上互联架构，实现全网资源的统一互联与灵活调度。

最后，全网启用 BGP 动态路由协议，实现路由信息的自动学习与动态传递，大幅降低人工维护复杂度。结合 BGP 路由策略，可依据实际业务需求实现智能流量调度与路径优选，增强网络拓扑的灵活性与智能化水平。

## 4. 收益效果

### 优势：

**链路层冗余，业务可用性提升至 99.99%：**

环形拓扑提供链路冗余，支持链路快速切换与故障自愈，显著提升业务连续性。

**动态路由减少手工配置，降低运维复杂度：**

BGP 动态路由支持自动学习与传递 VPC 路由，减少了人工配置与调整的风险，提升了运维效率。

**灵活的 BGP 路由策略，优化业务路径选择：**

通过多样化的 BGP 路由策略，支持不同业务流量的路径优化，全网流量调度更加灵活。

### 效果：

**业务连续性显著增强：**

通过环形拓扑与链路冗余设计，将业务可用性从 99% 提升至 99.99%，避免单点故障对业务的影响。

**网络运维效率大幅提升：**

动态路由配置减少了人工干预，降低了配置复杂度和运维出错率。

云上统一管理各 VPC 互联，简化了网络拓扑，提升了扩展性。

**业务路径调度更加灵活：**

BGP 动态路由使各业务流量能够根据网络状态动态调整路径，保障关键业务的服务质量。

B 企业通过环形冗余链路、BGP 动态路由与云骨干网的整合，成功构建了高可用的混合云网络架构。改造后的网络不仅解决了单点故障与配置复杂的问题，还显著提升了业务连续性与运维效率。未来，B 企业将继续优化网络架构，探索边缘计算与智能化网络调度方案，为业务创新与数字化转型提供坚实的网络基础。

# 三 某互联网企业通过云骨干网构建高可靠跨云网络

## 1. 案例背景

C 企业作为国内领先的社交娱乐平台服务商，旗下的语音平台覆盖千万用户，为游戏玩家与社交用户提供高质量的实时语音、聊天及娱乐服务。尤其在年度盛典等重大活动期间，语音平台需要承载数倍于日常的高并发流量，对网络的可靠性、灵活性和故障恢复能力提出了严苛要求。

## 2. 业务痛点

### 多云网络割裂，业务重复部署：

语音业务分布在多个公有云平台，网络之间缺乏统一的互联机制，导致业务需要在不同云上重复部署，增加了资源浪费与管理复杂度。

### 链路中断，切换缓慢：

跨云网络依赖单一链路，链路中断时切换流程复杂且响应缓慢，可能导致业务中断，影响用户体验。

### 故障切换，单线承压：

缺乏链路冗余和负载分担能力，故障切换后只能依赖单线承压，容易出现链路过载、延迟升高等问题，无法满足高并发语音通信需求。

## 3. 解决方案

为构建高可靠、智能化的多云互联网络，C 企业采用以企业路由器（ER）为核心的双链路冗余与动态路由架构，实现跨云网络统一接入与自动化故障切换。具体实施方案如下：

首先，实施双链路冗余设计。在现有跨云专线基础上新增 VPN 备份链路，依托企业路由器（ER）的链路互备能力，对专线状态进行实时监测。当专线发生故障时，系统可自动无缝切换至 VPN 链路，全程无需人工干预，有效保障业务连续性与可用性。

其次，启用 BGP 动态路由协议。通过 BGP 实现专线与 VPN 链路之间的动态路由切换与优化，确保业务流量始终沿最优路径传输，同时大幅提升故障场景下的路由收敛速度与网络恢复效率。

再次，构建多云统一互联架构。通过企业路由器将多个公有云平台的 VPC 及本地网络进行统一接入与互联，消除云平台间的网络隔离，实现资源整合与统一管理，为业务灵活跨云部署提供基础支撑。

最后，实施链路负载分担策略。在专线与 VPN 链路之间配置负载均衡机制，根据实时流量状态动态分配数据转发路径，避免单条链路出现过载，提升整体网络吞吐能力与资源利用效率。

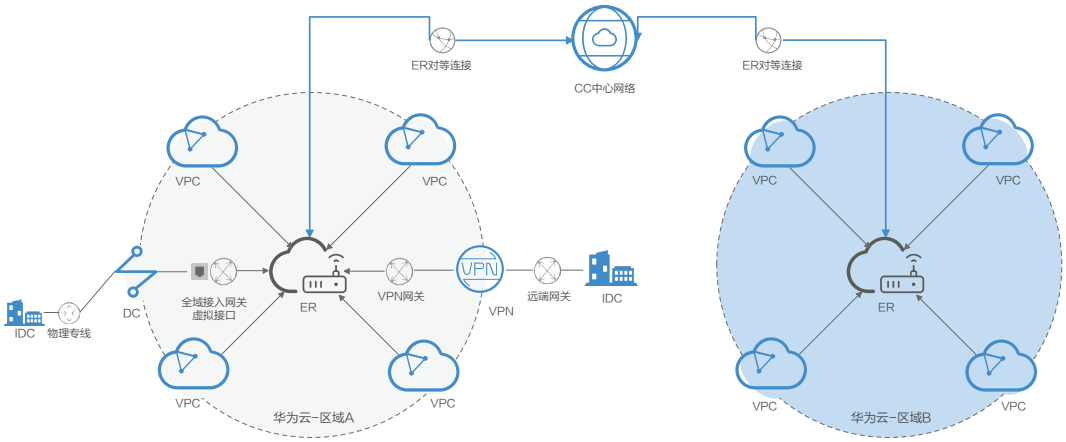



图 8 B 企业优化后组网图

## 4. 收益效果

### 优势

**链路冗余，业务连续性增强：**

专线与 VPN 双链路互备设计，保障了链路的高可用性，消除单点故障风险，实现业务连续在线。

**自动化切换，故障恢复更快：**

动态路由协议自动切换链路，切换时间从原来的分钟级缩短到秒级，显著减少因链路中断导致的业务中断时间。

**跨云网络统一互联：**

企业路由器打通多云平台网络，为业务提供一致的互联体验，提升资源利用率，降低重复部署成本。

**负载均衡，避免链路过载：**

专线与 VPN 链路之间的负载分担策略，保障了高并发流量下的稳定性与性能。

### 效果

**业务洪峰 6 小时 0 故障：**

在年度盛典期间，语音平台承载了数倍于日常的高并发流量，双链路冗余设计有效支撑了业务洪峰 6 小时 0 故障。

**千万用户优质语音体验：**

动态路由切换和智能负载均衡保障了语音通信的低延迟和高稳定性，提升了用户体验。

**运维效率显著提升：**

动态路由与链路冗余设计减少了人工干预，缩短了故障处理时间，并降低了运维难度。

**成本优化：**

通过跨云网络统一互联，降低了业务重复部署的资源浪费，实现了更高的资源利用率和成本效益。

C 企业通过企业路由器与双链路冗余互备方案，成功构建了可靠的跨云网络，实现了年度盛典期间的业务洪峰 6 小时 0 故障，保障了千万用户的优质语音体验。这一实践为其他企业打造高可用混合云网络提供了重要参考案例。

# 05 趋势与展望

面向未来，IT 基础设施正处于从“通用化”向“智能化”“业务原生化”加速演进的关键阶段。以人工智能为代表的新一代技术体系正深刻改变产业形态与企业运营模式，也对算力、网络、数据等底座能力提出更高要求。企业级云网不再只是基础设施配角，而将成为连接 AI 时代业务与算力的“第一公里”，其智能性、弹性、安全性和服务化水平将直接影响企业创新效率与数字化竞争力。

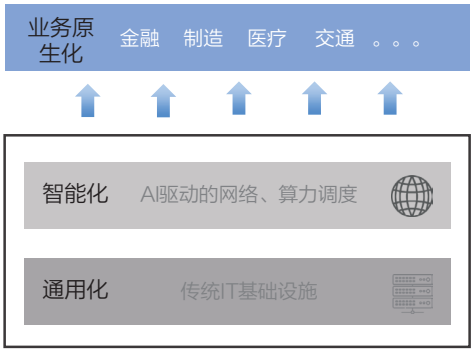



图 9 未来 IT 基础设施演进路径图

## 一 人工智能驱动多元业务场景的网络标准化

人工智能的广泛应用将催生多元化场景需求，并对网络能力提出更高标准：

**在金融领域，**智能风控、量化交易与跨境支付需要更低时延和更高安全保障；

**在智能制造领域，**工厂 AI 视觉检测、产线协同依赖边缘计算与毫秒级网络调度；

**在医疗健康领域，**远程手术与 AI 诊断要求大带宽、零丢包和全链路加密传输；

**在交通与低空经济领域，**车路协同与无人机调度需要网络具备实时定位、边云协同与广域覆盖能力。

这些场景的共性是：对算力与数据的跨域协同提出前所未有的要求。企业骨干网需完成从“静态连接”向“智能连接”的转变，具备大带宽、高稳定性和多路径容灾能力，成为 AI 场景下的数据与算力流动枢纽。特别是在“东数西算”与全国一体化算力网持续推进的背景下，骨干网将成为承接分布式智算节点、保障模型推理与多源数据协同的核心基础。

## 二 网络支撑能力走向智能化、就近化与可视化

未来企业级云网演进的核心特征，将集中在智能化、就近化和可视化三个方面：

**智能化：**基于 AI 模型进行动态预测和资源调度，实现“业务在哪，算力就调度到哪”，打破静态配置的局限；

**就近化：**通过云—边—端协同，让数据在靠近终端的节点完成计算，满足自动驾驶、高清视频、AR/VR 互动的毫秒级时延需求；

**可视化：**网络状态从“可监测”升级到“可理解、可预测”，通过拓扑感知、链路质量打分和流量标签化，实现业务级路径编排与动态优化，使网络从“黑盒”走向“透明化、运营化”。

这些能力的结合，将使网络不仅是“传输通道”，更是保障关键业务确定性与连续性的战略资源。

## 三 AI 技术深度赋能网络调度与运维体系

AI 已不仅是企业应用层的引擎，更在基础设施领域全面渗透，成为网络智能化演进的关键驱动力：

**调度优化：**AI 分析链路状态、业务行为和用户需求，实现实时路径推荐、故障预测与容量预判；

**智能运维（AI Ops）：**通过日志采集、异常检测与自动策略推送，构建“预测—诊断—优化—闭环”的自动化运维流程；

**主动安全防护：**结合零信任架构与 AI 威胁识别，实现动态权限验证、服务质量弹性分配与风险预警。

这将推动网络进入“自治化”阶段，即具备自学习、自优化和自愈能力，降低人工干预成本，提升系统韧性。

## 四 从“网络适配业务”迈向“网络感知业务”

企业级云网的价值边界正在持续外延，未来的网络不再是被动适配业务的通道系统，而将主动感知业务意图与上下文需求，成为数字业务的协同参与者：

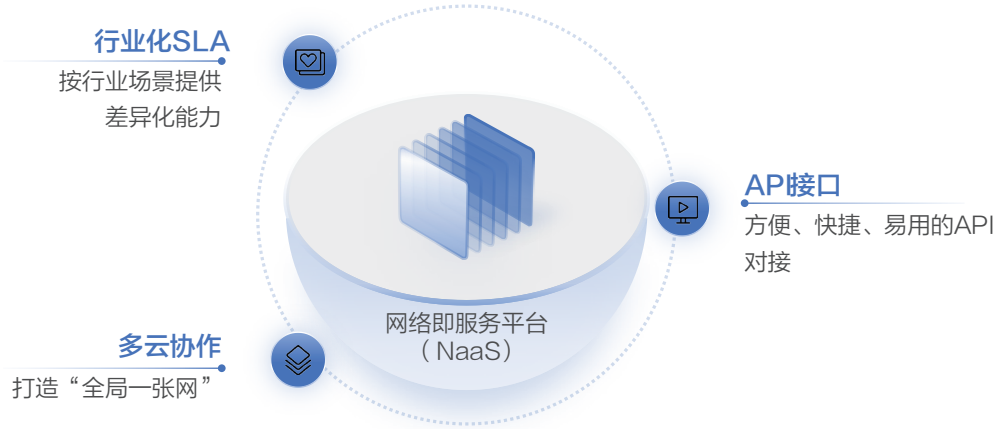



图 10 网络平台化生态图

**平台化：**网络能力以 API 接口开放，支持 NaaS（网络即服务），推动业务编排与自动化交付；

**跨域协同：**通过多云 VPC 互联和边缘节点联邦，打造“全局一张网”；

**差异化 SLA：**按行业场景提供专属能力，如金融级低时延高可靠、制造级实时性、医疗级高安全与合规性。

企业级云网不再是“后台支撑工具”，而将成为“智能业务平台”。在算力驱动逐渐让位于网络牵引的趋势下，云化骨干网将在数字化生态中发挥战略级作用，成为企业实现新质生产力跃升的核心抓手。