SD-WAN
V100R022C00
产品介绍

文档版本 01

发布日期 2023-02-27

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 趋势和挑战

随着企业IT向云架构的不断推进，以及公有云的崛起和流行，引导着企业数据中心等基础设施云化，越来越多的企业开始在公有云安家，从而打破企业IT的传统封闭架构，引领企业网络架构走向开放之路。与此同时，企业的关键应用也逐渐云化，依赖于应用服务商提供的SaaS服务（如Office、生产ERP系统、销售系统等），企业通过互联网从云端访问日常办公所需关键应用的趋势日渐明显。云化不仅仅是一场技术变革，也是商业模式的变革，但是企业分支的业务向云端迁移，面临的挑战依然不少。

- 传统WAN架构封闭：企业WAN难以实现多云多网互联

  数字化与全球化使得企业分支站点面临在更广地域、更多样化的运营商接入网络条件下实现快速互联，同时随着未来几年内，企业业务云端部署的形势加剧发展，企业的传统分支、总部和数据中心，还需要更加开放和灵活地连接到Internet、公有云以及SaaS应用。新形势下，如何高效、快捷地实现企业WAN的多网互联，承载企业庞大、复杂的组织和业务互联诉求，成为企业能否成功完成数字化变革的关键。

- 应用体验难保障：海量应用带宽共享，业务冲突导致体验不佳

  随着Internet的普及，其网络的覆盖范围和网络质量有了很大的提高，Internet成为许多企业除了传统专线之外新的重要选择，但是Internet网络本身并不保障服务质量。此外传统网络对业务不感知，无法获知应用的状态，当遭遇突发流量链路拥塞或质量劣化的时候，往往会造成关键业务体验无法保障。

- 业务上线周期长：传统方式难以满足业务灵活部署的诉求

  传统的专线新业务发放速度慢，从业务申请到开通往往需要长达1～3个月的时间。同时云化趋势下，企业业务更新发展迅速，当前网络难以满足快速上线和业务变更的要求。

- 网络运维难度大：设备类型多，手工命令行配置低效易错，业务流量不可视，运维效率低下

  传统模式下，需要专人到现场对设备进行维护，但随着企业分支跨地域分布越来越广泛，设备类型越来越多，设备数量激增，导致维护难度大、成本高。此外随着业务不断增多和业务云化，WAN网络中分支到分支、公有云、私有云的流向更加复杂，传统的网络运维方式已经难以适应业务的发展。

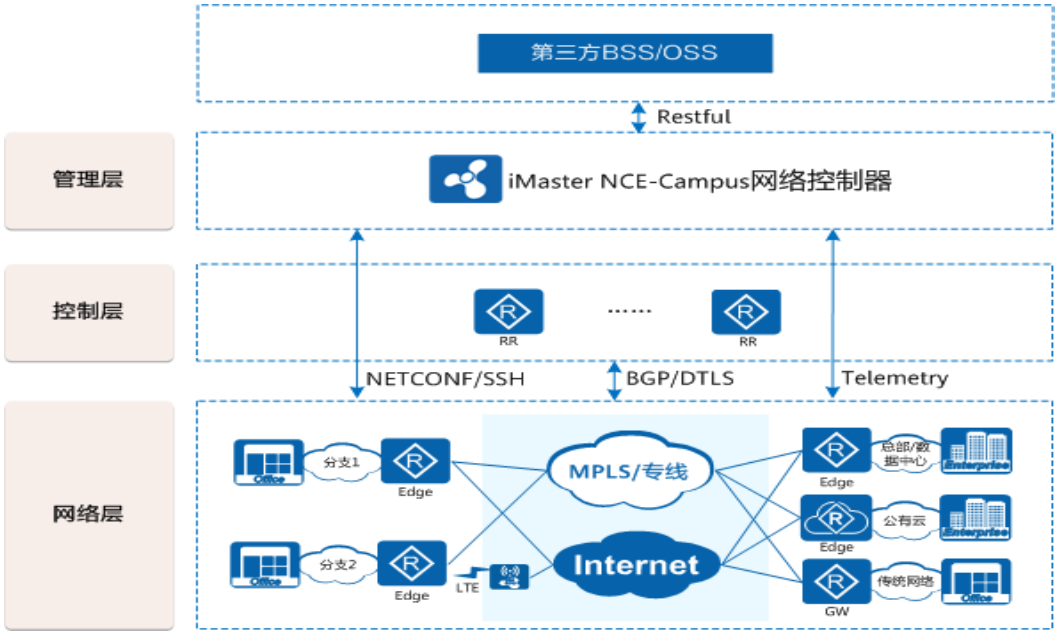
2 SD-WAN 解决方案

针对企业网络当前面临的WAN封闭架构、业务体验难保障、业务部署慢和运维困难的问题，华为SD-WAN解决方案为企业提供分支与分支、分支与数据中心、分支与云之间的全场景随需互联，并通过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。

SD-WAN 总体架构

华为SD-WAN解决方案总体架构如图2-1所示，主要包括：管理层、控制层和网络层。每层具备明确的核心组件并承担不同的功能。

图 2-1 SD-WAN 的架构



第三方BSS/OSS：当运营商或者企业客户希望将SD-WAN的端到端业务处理流程纳入到已有的BSS/OSS等第三方业务编排系统中时，可以借助SD-WAN网络控制器的北向开放API能力，实现对SD-WAN方案的集成和界面的灵活定制。

管理层

网络控制器是管理层的核心部件，是SD-WAN解决方案的智慧大脑，具有网络编排、管理能力，通过已有的Portal界面，进行SD-WAN端到端业务处理。

- 网络编排：负责SD-WAN面向业务的网络模型抽象、编排和配置自动化发放，主要包括企业WAN组网和各种网络策略相关的业务编排。网络控制器通过对企业WAN进行网络模型的抽象和定义，屏蔽了SD-WAN部署和实现的技术细节，使WAN网络配置和业务发放更加简易、灵活。
- 网络管理：通过网络管理功能实现了对企业WAN的网络层设备的统一管理与运维，主要包括统一配置网络业务；采集设备的告警和日志等故障信息；基于链路、应用、网络的性能数据采集、统计和分析；基于网络拓扑、告警管理、性能监控等方式多维度统计和呈现运维信息。

控制层

RR（SD-WAN Route Reflector，SD-WAN路由反射器），是控制层的核心产品组件，主要负责集中控制SD-WAN网络层的路由转发和拓扑定义。RR的功能主要包括：SD-WAN租户VPN路由的分发和过滤；VPN拓扑的创建和修改；站点间Overlay隧道的创建和维护等。相比传统网络完全的分布式控制方式，这种集中式的控制实现了企业WAN控制平面和转发平面的分离，简化了网络运维操作，减少了网络配置错误几率，提升了企业WAN的运维效率。

在实际部署时，RR即可以独立部署，也可以与已有的Edge站点共部署。

网络层

从业务角度来说，企业的分支、总部和数据中心以及在云上部署的IT基础设施等都可以统称为企业的站点。用于不同站点WAN互联的网络设备以及中间的WAN一起构成了SD-WAN的网络层。

从网络功能层次划分，企业SD-WAN网络可以分为Underlay网络和Overlay网络两层。

- Underlay网络：即物理网络，是由路由器等网络设备通过运营商提供的物理线路互联组成的WAN，常见类型有MSTP专线、MPLS VPN以及Internet等。
- Overlay网络：即虚拟网络，是通过引入IP以及软件技术，在同一张物理网络上构建出的一张或者多张虚拟的逻辑网络。不同的虚拟网络虽然共享物理网络中的设备和线路，但是虚拟网络中的业务与物理网络中的物理组网和互联技术相互解耦。虚拟网络的多实例化，既可以服务于同一租户的不同业务（如多个部门），也可以服务于不同租户，是SD-WAN网络层的核心组网技术。

从网络设备的功能定位划分，企业SD-WAN的网络层主要由Edge和GW两种类型的设备构成。

- Edge：是企业SD-WAN站点的出口CPE设备。Edge的本质是SD-WAN隧道的发起和终结点，也可以看做是SD-WAN网络的边界点。Edge之间的Overlay隧道可以构建在任意的有线或者无线的Underlay WAN网络上。
- GW：是联接企业SD-WAN站点和其他网络（如传统VPN）的网关设备。通过GW可以实现SD-WAN网络到企业传统网络、公有云网络的互通。

3 客户价值

华为SD-WAN解决方案可以给用户带来显著价值。

- 多云多网按需互联

  SD-WAN提供包括Hub-Spoke、Full-Mesh、Partial-Mesh等丰富的组网模型，根据网络规模可选择单层组网或分层组网，Hub-Spoke组网支持多Hub站点部署模式，Full-Mesh组网支持主备逃生站点；在分层组网中，负责区域和区域之间互联的边缘站点支持主备双站点增强可靠性。站点可以选择部署CPE单网关或双网关，支持10+种WAN接口采用多链路混合方式接入网络。支持部署vCPE作为云网关，实现企业站点和公有云互通，提供优质的SaaS、IaaS等云业务体验。提供灵活的传统MPLS站点互访模式，使传统企业网络可以平滑演进到SD-WAN网络。改进了传统企业网络只能通过集中模式访问Internet的问题，提供基于应用的策略调度，可选择部分或全部应用通过本地访问Internet。

- 无损应用体验

  采用首包识别技术、业务感知SA（Service Awareness）技术快速识别应用，支持通过自定义应用规则识别特殊应用。CPE设备通过监控应用所在链路的延迟、抖动以及丢包率实时检测链路质量。支持多种智能选路策略，包括基于应用质量选路、基于负载均衡选路、基于带宽利用率选路、基于应用优先级选路。三级QoS流量调度技术，保障关键应用带宽。支持多种广域网加速技术，实现基于应用的音视频优化、应用优化、TCP传输优化等广域网优化功能，为客户提供极致业务体验。

- 极简部署运维

  支持邮件开局、U盘开局、DHCP开局、注册查询中心开局、云站点开局的即插即用开局方式，对开局人员零技能要求。基于链路、应用、站点等不同维度的统计结果展示和导出，清晰呈现业务统计信息。通过iMaster NCE-Campus可以对CPE集中运维管理，支持VAS自动加载和业务链灵活编排，支持CPE设备在线升级、远程管理。iMaster NCE-Campus支持强大的日志告警功能，提供了丰富的设备集中管理手段、故障诊断和巡检工具。基于GIS（Geographic Information System）、拓扑的全网站点健康度可视化管理，实现海量分支的简易运维，降低现场维护支出。

- 开放生态

  iMaster NCE-Campus提供基于开放标准RESTful的API和第三方平台对接，实现客户对于SD-WAN方案的集成和界面的灵活定制。支持iMaster NCE-Campus云化部署、vCPE云化部署，实现企业轻资产运营模式。

- 完善的安全体系

iMaster NCE-Campus设置多级管理员权限，iMaster NCE-Campus、RR和CPE（包括普通CPE、vCPE）之间使用增强型双向认证，支持更换为第三方证书的安全机制，部署防火墙采用防攻击等措施保证iMaster NCE-Campus、RR的系统安全。CPE支持安全启动、证书安全存储，并提供对系统中可疑的CPE进行隔离处理，防止攻击者利用被盗CPE设备接入网络。采用基于SSH（Secure Shell）的NETCONF协议、基于SSL加密的HTTP2.0协议和IPSec协议对数据进行加密处理，保证数据在传输过程中的安全。支持ACL流量过滤、URL过滤、IPS（Intrusion Prevention System）、防火墙功能，满足业务安全需求。

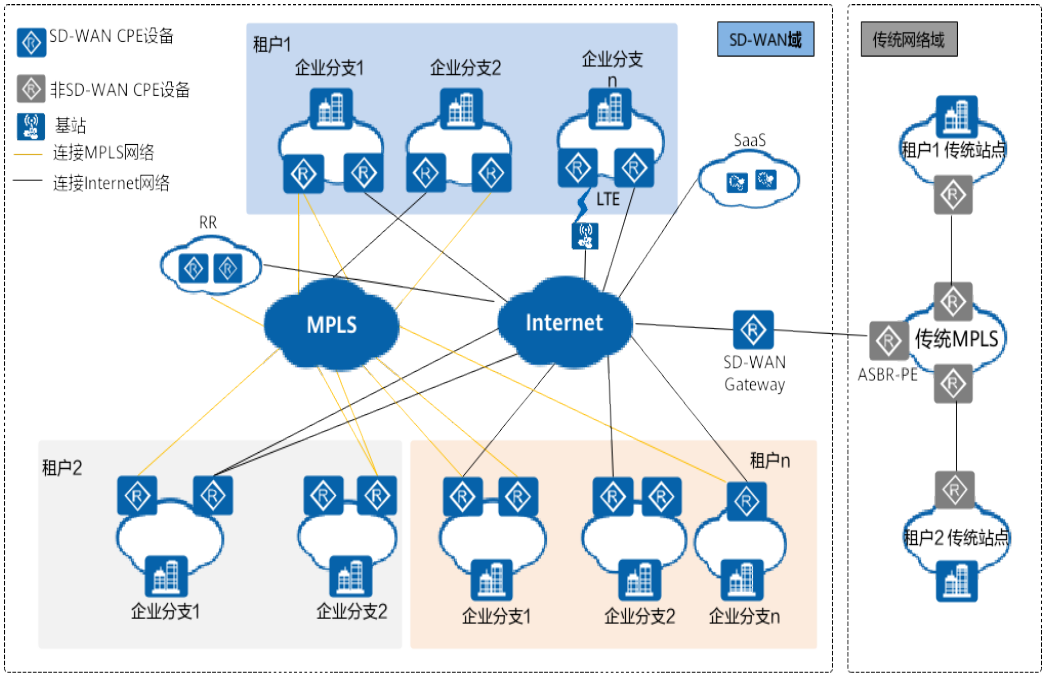
4 典型应用场景

华为SD-WAN解决方案主要场景可以分为运营商B2B业务场景和企业自建场景，企业自建场景根据企业规模又可以分为单层组网和分层组网场景。运营商B2B业务场景中，运营商在为企业客户提供方案时，也可以参考企业自建场景的网络设计方案。

4.1 运营商 B2B 业务

运营商需要为不同行业、不同规模的企业提供建设和运维企业网络的服务，使企业可以快速完成网络部署和业务开通。而且，运营商从网络管道提供商向服务提供商转型，为企业提供网络服务、增值服务、云服务等业务。

图 4-1 运营商 B2B 应用场景

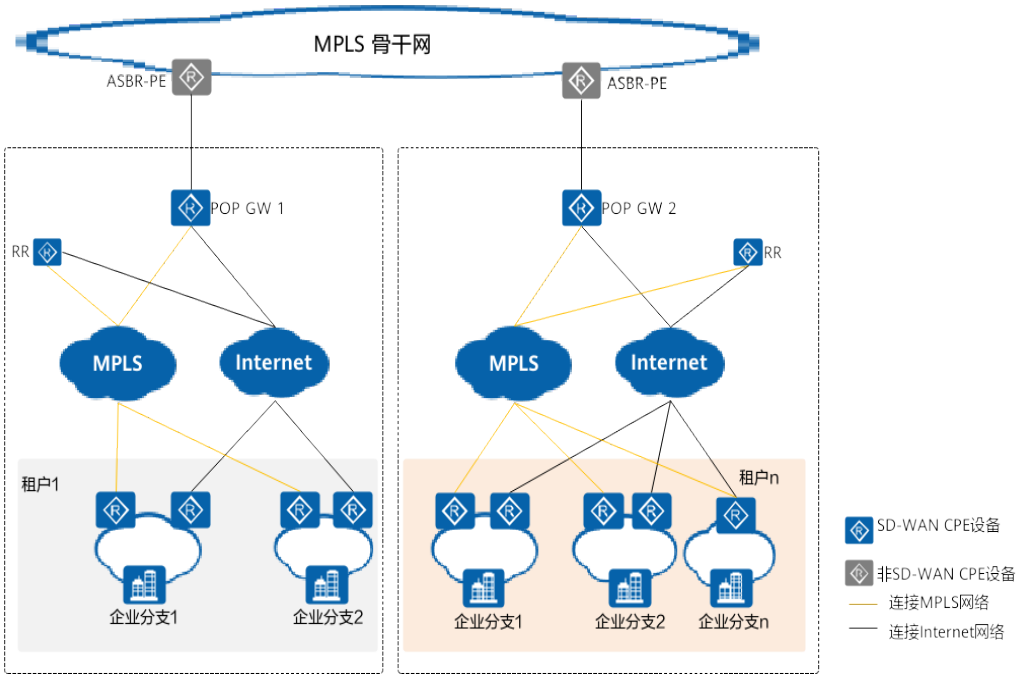


如图4-1所示，华为SD-WAN解决方案主要从以下几个方面提供解决方案。

- 运营商通过iMaster NCE-Campus多租户模式、部署支持多租户的RR设备，为多个企业提供SD-WAN网络。企业可以作为租户，租用运营商提供的SD-WAN网络，企业租户之间互不可见，每个租户独立维护企业自己的SD-WAN网络。
- 企业分支通过多种链路灵活组合接入网络，使用vCPE作为公有云和私有云的网关，实现和其他分支通信、访问SaaS应用，访问公有云和私有云。企业租户可以根据需求选择多级QoS策略，基于链路质量、应用优先级、带宽、负载均衡的智能选路，安全等策略，满足保障关键业务体验、高带宽利用率、安全等诉求。
- 运营商通过iMaster NCE-Campus的可视化运维系统，维护SD-WAN网络，统一部署管理云业务，为企业提供增值服务。
- 企业网络有客户资产的存量经营需求，需要支持SD-WAN站点和传统分支站点互访，运营商可以部署支持多租户的IWG设备与传统网络中的ASBR-PE（Autonomous System Boundary Router，自治系统边界路由器）设备互通，同时解决多个企业网络SD-WAN站点和传统分支站点的互联互通需求。

针对大型企业，若为了实现跨国或者跨越多个区域的企业站点之间的网络互通，企业往往会选择全球性的运营商专线或者Internet的方式进行总部分支组网互联。基于华为SD-WAN解决方案提供的POP组网方案，运营商在高品质的跨国/跨区域的WAN骨干网边缘建立POP点，并在POP点内部署SD-WAN的Gateway设备（POP GW），POP GW设备与运营商骨干网边缘网络设备（PE）互联；借助本地运营商的MPLS/Internet，在企业分支站点与POP点的POP GW之间建立Overlay隧道，从而实现跨国/跨区域分支之间的互联，如图4-2所示。

图 4-2 运营商 POP Gateway 组网

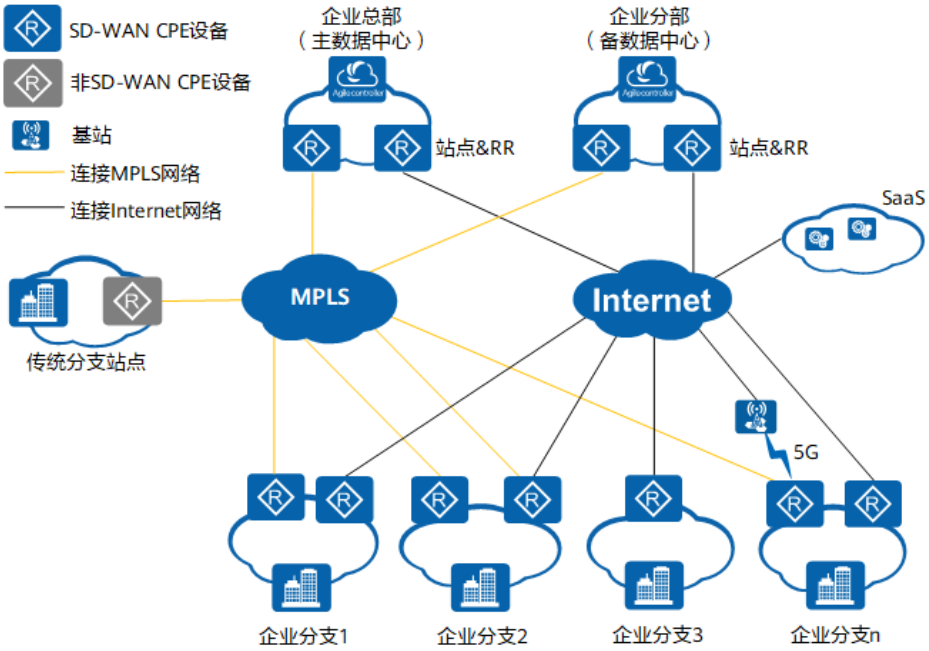


4.2 企业自建

对于实力雄厚的大型企业，可以选择部署一套自己的iMaster NCE-Campus系统，管理SD-WAN网络。大型企业有分支站点分布广、业务类型多样，对专线质量要求高等特点，面临业务流量爆炸式增长冲击专线带宽，关键应用体验差，运维困难等难题。大型企业的分支站点数量规模有两种情况，一种是分支站点数量少，且不存在跨国分布情况，推荐采用单层组网，如图4-3所示；一种是数量比较大（例如超过500个分支站

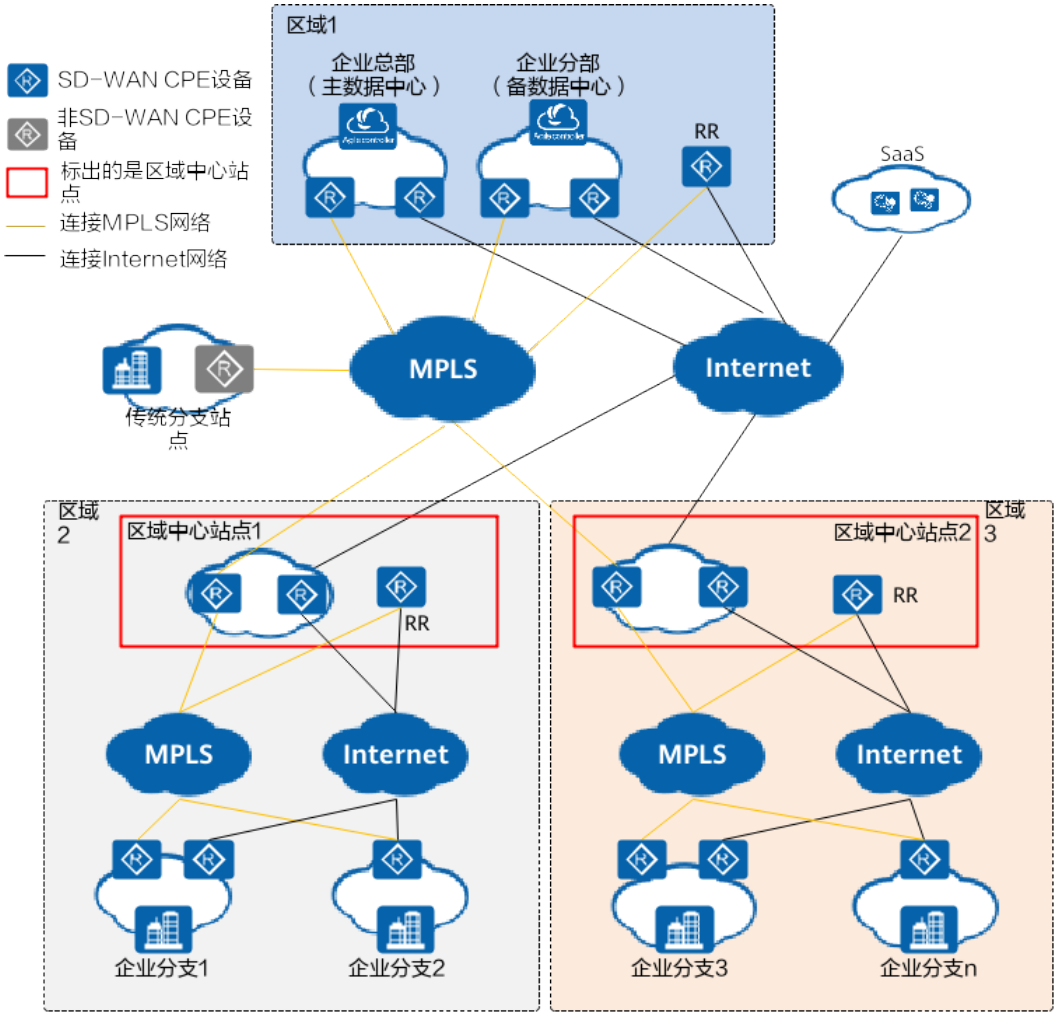
点），在一个国家广泛内分布在多个地域，或者虽然分支站点数量少但是存在跨国分布情况推荐采用分层组网，如图4-4所示。

图 4-3 单层组网场景



- iMaster NCE-Campus可以在数据中心部署，推荐使用异地容灾部署方案，保障控制系统高可靠性。
- 总部和分支可以采用双CPE网关MPLS和Internet混合链路接入网络，满足对专线的高质量要求，无法使用有线链路接入网络的站点，还可以采用5G接入网络。单层组网中的所有站点属于同一个Overlay组网区域，Overlay组网拓扑可以采用Hub-Spoke组网模型或Full-Mesh组网模型。RR设备可以采用共部署模式，由总部或大型分支站点的CPE充当RR设备。也可以单独部署RR设备，参见分层组网场景。
- 可以通过配置多级QoS策略、基于带宽、基于应用的智能选路，满足保障关键业务体验、负载均衡高带宽利用率等诉求。
- 如果企业网络中存在未迁移到SD-WAN网络的传统分支站点，可以选择同时和传统专线网络、SD-WAN网络站点互通的SD-WAN站点，作为与传统分支站点互访的网关，完成企业网络的平滑转型。
- 可以通过零配置开局，业务自动编排下发，对链路和业务的多维度可视化管理、丰富的故障诊断和巡检工具，来解决海量分支带来的开局难、运维难的问题。

图 4-4 分层组网场景



- 分层组网场景中的iMaster NCE-Campus部署，站点CPE接入WAN网络及典型业务、运维手段均和单层组网场景相同。
- 和单层组网不同的是，分层组网中的站点被划分为多个Overlay组网区域，每个Overlay网络区域可以选择各自的Overlay拓扑（Hub-Spoke或Full-Mesh）。RR设备推荐采用单独部署模式，每个区域单独部署RR，控制该区域内站点之间的路由交换。采用分层组网有利于网络扩展、减少站点访问网络时延的优点。

5 特性

特性	说明
灵活大规模组网	基于EVPN协议的隧道方案，引入独立的分布式控制组件RR，增加拓扑编排组件，实现每个VPN不同的拓扑编排功能，增大规模组网能力。
IPv4 over IPv6	在Underlay网络为IPv6时，站点LAN侧IPv4业务可以通过SD-WAN EVPN建立的overlay隧道互通。
基于应用的智能选路	凭借强大的应用识别引擎和链路质量探测引擎，实现了基于应用优先级、链路质量、负载均衡、带宽占用率的智能选路，选择最优链路进行业务转发，保障关键业务质量，充分利用带宽，实现负载均衡。
基于FEC技术的音视频优化	FEC（Forward Error Correction，前向错误纠正）技术通过配置流策略的方式，对报文丢包进行优化。FEC通过流分类拦截指定数据流，增加携带校验信息的冗余包，并在接收端进行校验。如果网络中出现了丢包或者报文损伤，则通过冗余包还原报文，从而提升音视频应用体验。
多路包复制（双发选收）抗丢包技术	发送端CPE对数据包进行复制，把原始包和复制包通过多条链路中的两条一起发送。如果一条链路上有丢包，则接收端CPE通过另一条链路上的冗余包还原，从而不用重传。适用流量小，可靠性要求高的业务，例如紧急呼叫，付款业务，工业场景PLC业务。
逐包负载分担是提升链路利用率的技术	逐包负载分担技术可以将单条流的报文分担到多条链路上，充分使用多条链路。在站点有多条出口链路时，可以加速大文件传输。适用FTP/HTTP下载大文件，数据备份等业务。
丰富的北向API	iMaster NCE-Campus支持丰富的北向API，满足客户对于SD-WAN方案的集成和灵活定制Portal界面的需要。
完全零配置开局	支持邮件开局、U盘开局、DHCP开局、注册查询中心开局、自动开局，网关设备自动注册到iMaster NCE-Campus，自动获取离线配置，完成网络部署。

特性	说明
全网应用质量可视	提供丰富的质量统计信息，可以实时查看站点内、站点间的链路质量、应用质量、吞吐量等情况，统计数据图形化动态展示，网络情况一目了然。
高性价比CPE	推出高性价比的NetEngine AR系列企业路由器款型。
简单易用的iMaster NCE-Campus系统界面	提供基于模板批量配置、导航式策略配置、页面简洁、表达丰富统计内容的iMaster NCE-Campus系统界面。
iMaster NCE-Campus集群系统异地容灾	支持在两个地域部署两套独立的iMaster NCE-Campus集群系统，系统之间建立心跳、数据通信链路，主集群的数据实时备份到备集群。在主集群发生重大故障无法恢复的时候，可以把备集群切换成新的主集群，从而继续提供业务服务。
Overlay隧道自动化编排	采用EVPN实现站点间Overlay隧道的动态建立，用户只需要完成Underlay网络的WAN侧链路配置和虚拟网络配置，iMaster NCE-Campus根据WAN侧链路配置自动完成隧道编排，无需用户手动配置，大大简化了网络部署配置。
多租户高性能GW	支持运营商部署多租户高性能的CPE作为GW设备，为企业租户提供与传统专线网络对接业务和POP组网业务。
系统安全部署	支持CPE的证书安全存储和证书更换、更新等安全机制；支持CPE与iMaster NCE-Campus、CPE与RR之间双向证书认证；支持CPE与CPE之间的数据平面中IPSec SA动态协商机制；支持对故障设备进行隔离。安全防护功能，支持IPS、AV、URL远程查询。
SD-WAN IPv6场景	支持在站点WAN侧为IPv4、IPv6或双栈的Underlay网络上构建SD-WAN网络，支持站点LAN侧部署IPv4和IPv6业务。
SD-WAN云部署	支持SD-WAN站点通过IPSec接入公有云VPN Gateway。支持Host VPC方式在公有云部署vCPE，支持Transit VPC方式在公有云部署vCPE。