**SD-WAN解决方案**

**华为技术有限公司**

**网络改造技术篇/成熟技术/工厂外网改造**

1. 概述
	1. 背景

伴随着企业的数字化转型以及云计算和SDN/NFV技术的兴起和普及，传统企业的WAN网络正在经历着深刻的变化。

传统的企业WAN网络通常租用运营商的物理专线或者MPLS VPN专线来实现企业分支的广域互联，保证网络的服务质量，因此企业WAN业务开通依赖运营商，业务开通时间较长且价格也比较昂贵，另外传统企业采取自建数据中心的方式来承载企业IT关键资产，企业网络架构是封闭的，开放性不足导致业务发放效率低。

随着Internet的普及以及云计算等新技术的兴起，传统企业网络架构正在经历革命性的变化，首先全球范围内internet的快速普及，无论从覆盖范围还是到网络质量，都有了质的提高，除了传统的专线互联技术外，Internet成为传统企业的分支互联以及全球化推进的一个新的重要选择；此外，云计算技术风起云涌，AWS等公有云的崛起和流行，引导企业DC等基础设施云化，从而打破了企业IT传统的封闭架构，引导企业网络架构走向开放之路，越来越多的企业选择公有云服务；此外，就是企业的关键应用的云化，企业的重要应用也逐渐被应用提供商改以SaaS云化方式提供，企业连接SaaS云业务逐年增长。

* 1. 实施目标

本解决方案的实施目标：

1. 零配置开局，设备即插即用；
2. 快速的发放连接业务，实现分支CPE即插即用以及园区/分支和云的按需快速互连；
3. 借助低价值的Internet链路进行更广泛的互联并且保证关键应用的体验不受影响；
4. 能够以云的方式提供管理手段，让企业用户更加方便快捷的自助定义新业务和进行网络管理。
	1. 适用范围

SD-WAN解决方案帮助制造企业实现未来较长一段时期的SD-WAN业务运营需求，主要包含如下场景的网络访问服务：

1. 零配置开局，设备即插即用
2. Site to Site访问：为企业客户提供企业分支之间的互访服务。
3. Site to Internet访问：为企业客户提供企业分支内到Internet的访问服务（含安全策略管理）。
4. Site to Legacy Network：为企业客户提供企业分支到传统网络（非SD-WAN网络）的访问服务。
5. 基于应用/应用质量的智能选路：如关键业务走高质量专线、普通业务走低质量；同时可以互为备份
6. 支持基于链路、应用、流量的可视化分析
	1. 在工业互联网网络体系架构中的位置

SD-WAN解决方案适用于图1中6，7，8场景。基于本解决方案提供的高可靠、低时延的数据传输保障，并通过应用级智能选路与智能加速、VAS业务随需获取和智能运维，构建极致业务体验，重塑企业专线全流程的业务体验。可以减少数据传输线路的部署、适用于多种环境以及设备移动的场景。



**图1 工业互联网互联示意图**

1. 需求分析

由于业务云化，工业制造企业需频繁与工业云互动，这就需要更高的网络带宽，为了保证服务质量，工业制造企业WAN 网络互联通常采用运营商MPLS 专线，虽然专线网络质量有保障，但价格过于昂贵，平均占企业OPEX 达50% 以上，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 成为许多工业制造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；云化趋势下，工业制造企业业务更新发展迅速，当前网络难以满足快速上线要求；传统专线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，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。

1. 解决方案
	1. 方案介绍

SD-WAN解决方案主要包含以下创新点：

1. 全场景互联

支持MPLS、Internet 等多种类型WAN 链路（xDSL, LTE/4G 等）灵活捆绑；提供支持单/ 双CPE、单双Hub、SaaS 接入等丰富的组网接入，实现低成本的Internet 链路与专线链路的混合接入；支持云端部署 vCPE，优化云业务访问体验。在保证关键业务质量的同时可节省50% 的广域网带宽租用成本。

1. 应用体验优化

支持6000+ 已知应用识别，并可以通过用户自定义应用，灵活识别行业特殊应用；通过IP FPM 链路检测、SPR智能选路、三级QoS流量调度等技术，实现业务智能感知和应用的智能流量调度，优先保障关键应用优质体验；通过传输优化、应用优化等多种广域优化手段，实现关键应用智能加速，提升和业务体验。

1. VAS 业务随需

基于X86/ARM 架构的系列化开放uCPE，覆盖不同规模的分支场景；支持10+ 业界主流VAS （vFW、vWoC 等），业务按需扩展；VNFs 全生命周期管理及业务链自动化编排，VAS 业务分钟级获取。

1. 智能运维

邮件、U盘等多种开局方式，设备即插即用；业务策略配置、增值服务编排及VPN 动态连接等全业务自动化配置，简化分支网络部署；应用与链路的可视化管理，自定义报表按需呈现，支持故障预知及快速定位。

* 1. 系统架构

本解决方案的总体架构如图2所示：



**图2 SD-WAN解决方案总体架构**

业务呈现层：

1. 面向运营商、MSP、大企业的自研Portal；
2. 提供业务灵活定制化界面。

网络编排/控制层：

1. 网络控制平台(SDN Controller) – 华为Agile Controller，完成网络业务编排以及网络业务发放；
2. 北向支持开放API接口，实现业务快速定制和自动发放；
3. 南向支持Netconf/Http2/SNMP等接口，统一管理控制物理和虚拟网络。

网络层：

1. 由物理和虚拟设备组成的企业WAN的基础物理组网, 主要包括uCPE/vCPE,vFW，第三方VAS等；
2. 基于DSVPN隧道提供灵活Overlay组网。
	1. 网络拓扑设计

SD-WAN Site:企业的办公场所或者关键IT设施部署点，业务上需要彼此通过WAN网络互联，实现互访：

1. 每个站点通常具备一个或者多个出口CPE，不同站点的CPE通过IP Overlay隧道方式进行互联；
2. 常见的站点类型：企业分支、园区、DC、公有云VPC。



**图3 SD-WAN解决方案拓扑结构**

* 1. 功能设计



**图4 SD-WAN解决方案全家福**

SD-WAN解决方案产品主要包含AC控制器、CPE/uCPE、vCPE、 VAS (vFW、第三方VAS）组成，各部件功能简介如下：

**表1 EC-IoT解决方案组成**

|  |  |  |
| --- | --- | --- |
| **部件** | **产品** | **功能说明** |
| 控制器 | Agile controller-Campus | 1、网络基础服务/南北向标准化，开放对接第三方构建生态系统2、面向商用，构筑高可靠性/高性能/安全性 |
| VAS | 包含：华为自研vFW：USG6000v第三方软件，如riverbed的广域加速等 | 虚拟化网络功能，独立软件 |
| CPE | AR系列的传统CPE，如AR161EW，AR3260 | 传统AR设备支持向SD-WAN演进 |
| uCPE | AR3600系列，AR650系列 | 可安装VNF的CPE设备 |
| vCPE | AR1000V | 1、架构领先：AR1000v支持单VM单vCPU和单VM多vCPU绑定方式2、性能强劲：单VM多vCPU部署方式，转发进程和安全进程独占vCPU，可显著提升系统的性能3、兼容性强：可运行于KVM、FusionSphere和Vmware vSphere等多个平台 |

* 1. 安全及可靠性

SD-WAN端到端安全解决方案：



**图5 SD-WAN解决安全解决方案**

综上所述，通过确保集中的管理控制系统(控制器)的安全性、用户接入设备(CPE)的安全性、用户业务隔离以及报文数据安全性以及用户接入SD-WAN网络的安全性，确保SD-WAN解决方案系统的机密性、完整性、可用性和可追溯性，从而保证整个SD-WAN解决方案业务的安全和正常运转。

* 1. 开放性设计

本解决方案符合SDN的目标，即将管理和控制功能与数据平面网络分开。这个目标的一个关键因素是开放性，以确保整个生态系统的互操作性。

1. 敏捷控制器北向接口通过Restconf接口（RFC6020，draft-ietf-netconf-restconf-03（Yang））与Orchestrator进行通信，并通过传输层安全（TLS）传输。
2. SDN解决方案支持OpenFlow，OVSDB，SNMP，Netconf，PCEP，IGP，BGP-LS等覆盖和底层组网的多个南向接口，当与网络基础设施接口时，SDN控制器使用YANG模型的接口和参数，可以根据需要非常灵活的创建新策略，修改原始策略。
3. 敏捷控制器实现了全面的Neutron API接口，可以与标准的Openstack和自有的Openstack分布式Fusionsphere集成。在Openstack社区提供ML2驱动，L3代理，FW和VPN插件。这些插件或驱动程序提供网络，子网，端口，安全组，路由器，EIP，SNAT和IPSEC VPN等的管理。
4. 成功案例

SD-WAN解决方案在日本软银，瑞士电信等项目中规模部署。