易科腾
EQTINFO

ANP SD-WAN 5.0
技术白皮书

2024年7月

易科腾

ANP SD-WAN 5.0技术白皮书

文档名称	ANP SD-WAN 5.0技术白皮书
版本号	V5.0
拟制人	
发布日期	2024-7-31

1. 术语和缩略语

本文档所使用通用术语、缩略语请参见《产品研发术语和缩略语》，专用术语和缩略语参见下表。

序号	术语/缩略语	英文含义	中文含义
1	ANP	Autonomous Network Platform	自治网络平台
2	ASG	Access Security Gateway	安全接入网关
3	CPE	Customer Premise Equipment	用户前置设备
4	gRPC	google Remote Procedure Call	谷歌远过程调用
5	LAN	Local Area Network	局域网
6	LCA	Local Control Agent	本地控制面代理
7	NAT	Network Address Translation	网络地址翻译
8	NVE	Network Virtualized Edge	网络虚拟化边缘
9	POP	Point Of Presence	入网点
10	RPC	Remote Procedure Call	远过程调用
11	SDN	Software defined Networking	软件定义网络
12	SD-WAN	Software defined WAN	软件定义广域网
13	VPC	Virtual Private Cloud	虚拟私有云，一般指公有云的一个租户网络
14	VPN	Virtual Private Network	虚拟专用网
15	VXLAN	Virtual Extensible LAN	虚拟可扩展局域网
16	ZTP	Zero Touch Provisioning	零接触部署
17	PQC	Post Quantum Cryptography	后量子密码
18	QKD	Quantum Key Distribution	量子密钥分发

2. 背景

企业的业务发展内在需求、商业环境变化和技术的发展三种力量驱动了企业广域网的持续演进。

- 企业因业务发展需要快速地在特定区域乃至全球范围内扩展门店和分支机构。企业自身专注于主营业务的拓展，包括将企业的IT系统快速延伸到分支，而不希望受运营商网络接入条件的限制，希望能够统一融合本地、互联网、云资源和安全平台，在混合和多云组网环境中提升运营效率、一致性和可扩展性，支撑企业广域网的数字化转型。
- 企业业务的全球化拓展和信息化程度的加深，企业的广域网络连接着众多的分支机构、远程办公人员和合作伙伴，大量的敏感信息，如客户资料、商业机密等，都在这个网络中流转，任何安全漏洞都可能给企业带来不可估量的损失，因此，企业广域网需要保证数据传输过程必须得到严格的安全、全面、有效的保护。
- 远程办公、线上会议等新形式的工作方式兴起，有效提升了企业内部跨地域部门、和外部客户沟通效率，也大幅降低了差旅成本。这就使得企业需要一种低成本的在任何地点、任何区域都可以安全接入企业私网的网络连接方案。
- 企业业务愈加复杂，不同应用的网络传输路径和网络质量诉求参差不齐，广域网需要提供灵活的应用识别和调度能力，可以针对关键应用进行优先级排序和优化，提升用户体验。
- SD-WAN(软件定义广域网)是一种提供企业广域网便捷连接技术，并且随着时间的推进，不断演进、深化。从最初的自动化的企业虚拟专网连接，演进到包含虚拟专网连接、边界安全防护、广域网络优化的三位一体解决方案。

3. 易科腾ANP SD-WAN系统

3.1 易科腾 ANP 系统的设计理念和客户价值

易科腾ANP SD-WAN的愿景是将企业专有网络延伸到全球范围内任何有网络连接的地方，构建无边界的企业网络，并保证足够可靠、安全。所以ANP系统可以充分利用一切已有的连接技术接入企业私有网络，包括MSTP/OTN专线、MPLS线路、有线上网宽带、4/5G移动网络，乃至卫星线路，支持按应用需求的多链路按质量择优选路、QoS优化来保证关键应用的体验。同时支持通过集中管控的微分段安全策略在无边界的网络上构建安全防护边界。

易科腾ANP产品诞生之初就是一个完全面向运营级SD-WAN场景设计、优化的产品，采用了大量的创新技术来保证SD-WAN的客户体验，而不仅仅是已有产品、开源组件的拼凑。ANP的设计理念包括：

- 原生的运营级多租户网络架构，从SD-WAN编排模型到控制器、POP设备、CPE设备都原生支持多租户架构，转发平面采用VXLAN或者VXLAN Over IPSec封装，以支持大规模SD-WAN运营场景以及大型企业客户的多网络平面隔离和分权分域管理需求。
- 极致的轻量级、易用性设计，裁减掉不必要的特性，让系统在绝大多数场景下足够用且好用，让系统消耗更少的IT硬件资源、更少的人力维护成本。
- 极致的传输安全特性，系统提供多层次、全方位的传输安全加固；首先，CPE内置应用识别DPI引擎，针对应用进行细粒度的识别和QoS策略调度；其次，基于业务链模型加载IDS/IPS组件，对潜在安全流量进行清洗，并进行阻断；在业务隧道封装传输阶段，可以启用端到端加密，保证数据传输在运营商网络不落地；最后，CPE通过PQC抗量子算法+QKD（量子密钥分发）对密钥协商过程进行强化，保证数据加解密的信息论安全。
- 专有的WAN优化隧道，提供双发选收、FEC、丢包重传、数据压缩等丰富的应用优化技术，针对视频、语音等业务进行精准识别和应用体验优化，提升底层链路带宽、降低丢包率。
- 将研发、生产流程的软件灌装、上线运行和业务开通统一拉通考虑，插上SIM卡即可用接入网络。易科腾为每个CPE颁发唯一的证书，用证书公钥的Hash值作为CPE的认证标识，CPE上电后根据证书查询注册服务器，注册服务器中登记CPE对应的控制器，最终和控制器完成基于证书的认证，并下载配置数据，从而完成真正的”零配置”上线。
- 轻量化的All-In-One设计。即使是数百元的低端CPE上，也包含了多租户的VPN连接、微分段安全防护/基本上网行为管理和应用识别优化功能。并且一台设备可以替代几台完全不同的设备，不仅减少了购买成本，更重要的是ANP系统可以全面支持集中的网络及安全策略管控，大大降低IT人员的运维难度。
- 控制器和CPE/POP之间采用高效的gRPC接口，统一支持配置、监控和路由通告等功能，从

而可以支持数以十万计的CPE组网场景。并且我们将源自于P2P大规模分布式系统中的Merkle树对账机制引入到ANP中，并通过gRPC接口原生支持Merkle树的对账流程。

3.2 ANP 5.0 SD-WAN 系统构成

3.2.1 网络架构及产品简介

ANP 5.0 SD-WAN系统内置了IPSec VPN加密、安全防护和广域网优化能力，全面支持IPv4/v6双栈组网。其系统架构如图 3.1所示，包含了如下组件：

- ANPC控制器，负责全网设备的接入认证和业务控制，北向开放全部gRPC和REST API。南向采用自定义的gRPC协议控制CPE/vCPE/vPOP设备，也支持NetConf和第三方设备对接。支持三节点集群部署。
- ANPM管理器，负责全网设备的管理、监控，一般和ANPC合一部署，也可以分离部署。支持多租户管理，支持账户的分权分域权限管理。
- ASG1200系列接入CPE设备，用于门店、分支的接入，全面支持Wi-Fi和4G，其中部分款型支持5G，可配套国密加密卡。软件功能支持L2/L3转发、多VRF隔离、OSPF/BGP动态路由协议、SNAT/DNAT、VXLAN&VXLAN Over IPSec、安全组微分段隔离、PBR、链路质量检测、基于应用识别的QoS调度/SLA链路选择/上网行为管理等等。支持HA双机部署。
- ANP SD-WAN客户端软件，用于PC客户端的拨号接入。
- ASG2000系列，总部硬件接入和汇聚设备，可配套国密加密卡，和ASG1200的功能基本一致，并且性能更加强大、网络接口更加丰富。
- ASG2000v，其充当两种角色：1）vCPE软件，以虚机形式部署，用于接入企业的私有云或者公有云VPC网络。2）vPOP软件，部署在专门的汇聚数据中心或者公有云上，提供全网的连接汇聚。

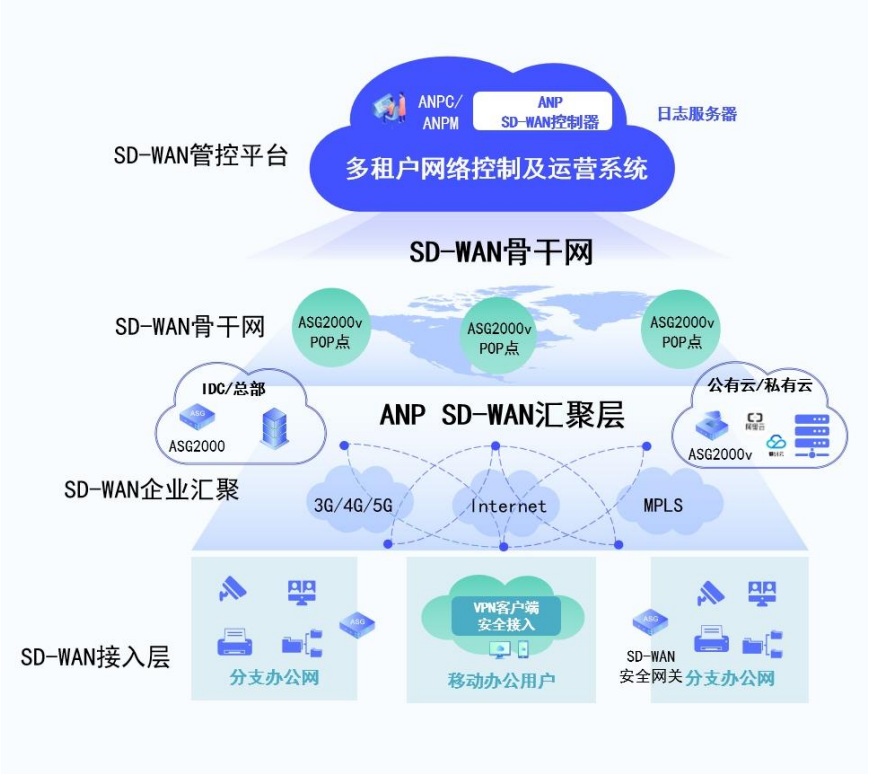


图 3.1

3.2.2 ANP 软件架构

ANP系统软件架构见图 3.2所示，自上而下由ANPM(管理及编排器)、ANPC控制器、ANP-OS软转发平台构成。其中ANPC+ANPM可以合一部署，在200个CPE的网络规模下，消耗系统资源不超过4核vCPU+8G内存，最低可以在2vCPU+4GB RAM的系统下运行。

ANP-OS可以运行在全系列的基于ARM、x86 CPU的CPE硬件上，也可以部署在虚拟机中。最小资源消耗仅为2vCPU、512MB RAM。

ANP-OS 5.0基于RUST对硬件管理模块进行重构，将软件系统与硬件适配层解耦，进一步提升产品性能和安全性，同时极大缩短新品CPE的导入适配周期，对于任意一款新硬件，在驱动及Linux小系统已经就绪的情况下，1周时间内完成适配。

ANP控制器采用轻量级、微服务架构，管理控制分开，可以实现控制器的3节点集群部署和异地容灾；对于超大规模的全球性网络，控制器可采用分层方式，实现超级控制器和域内控制器的分层控制，可扩展性强。

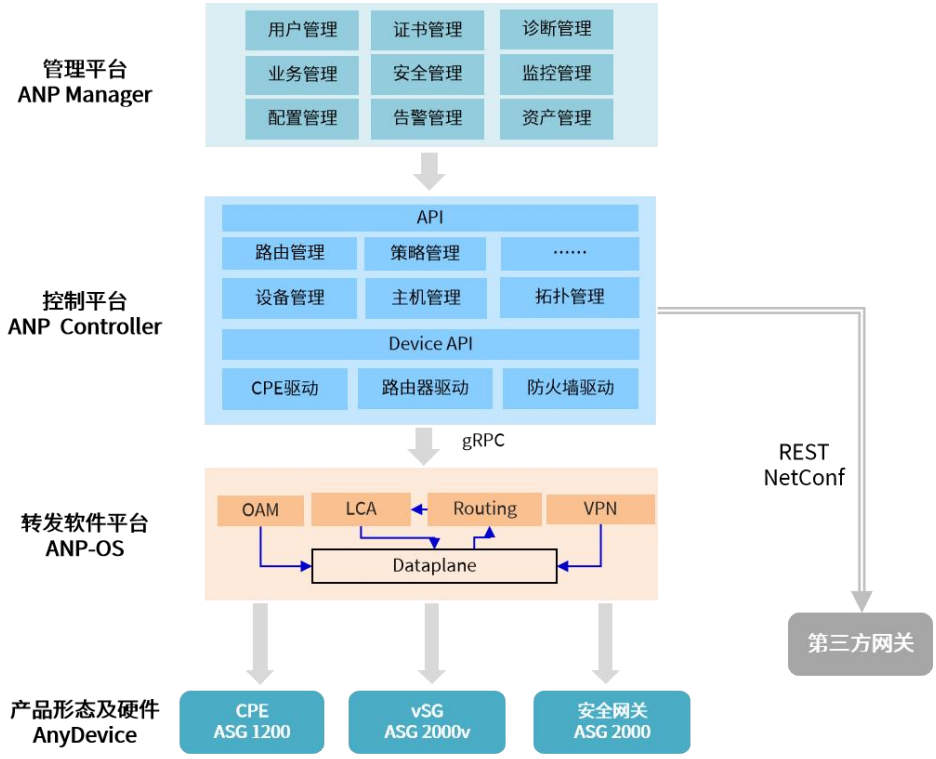


图 3.2

3.3 ANP 支持的组网模式

3.3.1 统一POP汇聚的Hub-Spoke/星型组网方式

- vPOP充当Hub节点，汇聚所有的CPE流量，vPOP本身完全是多租户架构，采用VRF做租户流量隔离，单个POP最大支持4000个VRF。
- CPE/vCPE充当Spoke节点，Internet流量默认本地出口，私网流量通过VXLAN Over IPSec隧道发送到vPOP节点进行路由。也可以配置PBR策略路由或应用识别策略，将Internet流量也通过私网统一出口。CPE支持和企业内部网络运行OSPF/BGP路由协议，接收路由通告，并通过控制器发布到其它分支机构，同时对于控制器通告的路由表项，也支持通过路由协议通告给企业局域网内的路由/交换设备，即使企业出口位于NAT之后，动态路由的能力也不受影响。

  易科腾ANP也支持POP的多跳、层次化组网，控制器支持POP之间的最短路径计算。

3.3.2 总部CPE直接汇聚分支的星型组网方式

ANP SD-WAN架构支持CPE和POP能力的合一，既可以汇聚流量，也可以处理正常的广域网出口流量业务。因而在SD-WAN私有化部署的情况下，可以无需部署专门的流量汇聚POP/vPOP设备，而是直接采用总部出口的CPE硬件来汇聚分支机构的VPN连接。

3.3.4 Full-Mesh组网方式

ANP支持两种Full-Mesh组网:

- 不加密VXLAN直接互联方式，适用于MPLS专网全互联的场景。可以通过将CPE配置为NVE，自动在租户内的NVE节点间建立Full-Mesh的VXLAN连接。
- VXLAN Over IPSec Full-Mesh互联，通过将租户内部的节点编排为对等的客户节点&服务节点合一角色，从而支持Full-Mesh的互联。

3.3.5 SD-WAN客户端软件接入组网

在ANP架构下，SD-WAN客户端就是一个轻量级的vCPE，其帐号开通、认证由ANP控制器统一负责，同时需要安装专门的易科腾客户端软件。

易科腾SD-WAN客户端软件拨号时，首先和控制器联系，控制器为其指派合适的POP点进行接入，可以基于双因子实现身份认证，零信任安全授权。在SD-WAN客户端接入的情况下，POP点同样支持多租户。

4. ANP SD-WAN的创新特色

4.1 基于数字证书的 ZTP 零部署和设备安全认证架构

如 图 4.1所示，易科腾CPE出厂时即分配唯一的序列号(SN)，并灌装唯一的证书(以证书的公钥的Hash值作为DeviceId，用于认证时识别身份)，这些信息通过生产文件提供给硬件工厂生产和灌装软件，同时录入官网注册服务器。当客户开通时，在官网登记客户的实际控制器地址。CPE发货到客

户处上电，只要DHCP可以获得地址，其自动查询易科腾官网的DNS，并向官网查询本CPE的实际归属控制器，官网返回结果，CPE再和实际的ANP SD-WAN控制器联系，认证通过后进行配置数据的下载。下载完成后即可以正常运行。

这些设计保证了在Underlay可以访问Internet的情况下，ANP SD-WAN是真正的ZTP免配置部署，在分支端，装维人员唯一要做的事情就是连接正确的网线、将CPE上电。

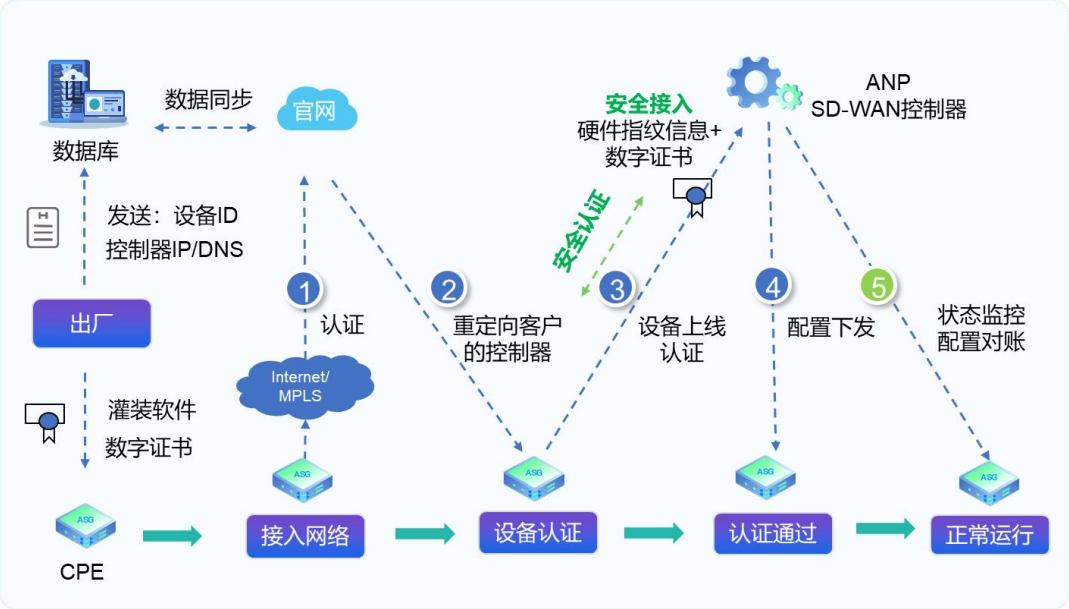


图 4.1

4.2 云原生的多租户架构

ANP从ANPM/ANPC控制器到POP设备、CPE，均原生支持多租户架构，兼容OpenStack Neutron的网络模型，转发采用VRF隔离。也支持单租户多VRF，方便同一个租户采用不同的网络平面隔离不同的内部业务系统。

控制器在多租户的基础上，支持基于角色/资源的授权，从而支持灵活的分权分域管理方式，以满足客户复杂的网管权限控制要求。

4.3 All-In-One 的灵活、通用的软件架构

易科腾采用统一的轻量级转发面软件系统ANP-OS，通过统一的硬件管理组件实现系统运行环境

初始化、转发系统参数初始化、4/5G模组、LED点灯的统一配置，后续系统软件适配无需关注硬件平台差异性，系统可以适配于任何硬件、市面上的任何4/5G、WiFi模组，大幅扩展产品使用场景和客户群体，全系设备将VXLAN/VXLAN Over IPSec、微分段安全/基本上网行为管理、应用识别、WAN QoS优化作为基本功能，路由协议可以裁减。从而可以在数百元的低端ARM平台上也可以支持全面的企业广域网边缘功能，并且这些功能都可以通过控制器进行集中的策略管理。

4.4 远程办公和 SD-WAN 统一接入

易科腾目前提供全平台的客户端软件，支持国产化操作系统和硬件平台。客户需要下载专门的SD-WAN客户端软件，并申请帐号才能接入网络。ANP系统可以统一管理远程办公的帐号、密码，也支持客户端软件在界面上本地修改密钥。客户端软件和vCPE接入一样，也支持多租户接入网络。

客户端软件下载后需要激活，ANP系统可以配置限定远程办公帐号和PC客户端硬件的绑定关系，以确保即使远程拨号帐号泄露，也不会造成安全泄密事件发生。

4.5 基于 PQC+QKD 的混合量子保密方案

易科腾ASG系列CPE基于国密算法叠加量子密钥协商功能实现端到端的量子保密通信，满足数据传输的信息论安全，可抵御量子计算的攻击；产品支持多种量子密钥协商方案：

- 基于直连光纤网络的QKD：CPE直接对接QKD设备，基于光量子偏振实时协商秘钥
- 基于PQC算法实现后量子时代数据安全加密：后量子密码PQC主要指抗量子计算的非对称密码算法，CPE可以通过软件升级支持，无需额外的软硬件投入；PQC可以取代IKE协商过程中使用的DH等公钥算法，在密钥协商阶段可抵御抗量子攻击。

4.6 高性能硬件加解密技术

易科腾CPE硬件主要分为X86和ARM架构平台，其中X86平台网络 SoC 处理器平台集成了 Quick Assist Technology (QAT) 引擎，

驱动软件实现与 DPDK、OpenSSL 等开源网络协议栈的整合，其中高性能汇聚设备ASG2000-S搭载英特尔灵动P5000系列CPU，基于第三代英特尔® QAT 加速器提供超25Gbps加解密性能，国密加密解性能超20Gbps，达到业内领先的水平。

易科腾ASG2000v软件系统在云环境部署时，可利用AES-NI指令加速，至强CPU上可以达到3Gbps/vCPU；同时为适应国产化和密评、密改要求，易科腾推出满足信创和国产化要求的CPE型号，目前主要包括：接入侧ASG1200-G1、汇聚侧EQR2000-XG/XG2等设备型号，同时全系SD-WAN CPE可配套易科腾自研EQD系列商用密码卡，密码卡提供标准PCIE、M.2、MiniPCIE等多种接口形态，支持DPDK驱动，最大可提供3Gbps 国密IPsec VPN吞吐能力，是高性能国密场景下、高性价比的配套CPE和SD-WAN解决方案的理想加解密硬件平台。

4.7 IPv6 功能的全面支持

ANP SD-WAN系统提供了完善的IPv6的功能，并且支持如下特性：

- IPv6 VPN能力：支持基于IPv6隧道承载用户v4/v6业务，支持的隧道类型包括IPSec、GRE、VxLAN、VxLAN over IPsec等，支持灵活的4in6、6in4等隧道封装；
- IPv6过渡技术：支持NAT46/64、DNS46/64、MAP-E/T、Ds-lite等IPv6过渡技术，兼容现网网络协议栈，平滑过渡，无需网络改造；
- 高级IPv6特性：基于IPv6扩展头部实现IFIT随流检测，支持基于BGP EVPN的SRv6 BE和TE Policy，支持EVPN VPWS/VPLS over SRv6、EVPN L3VPN over SRv6等

4.8 应用识别及智能选路

ANP SD-WAN方案支持基于五元组、域名以及DPI方式识别应用，并将多个应用聚合到应用分类中，在应用分类上挂接策略，这些策略包括允许/禁止访问、QoS优先级、带宽限速、SLA应用选路、强制重定向。同时支持客户自定义应用识别规则和新的应用分类。

对于SLA应用选路，支持定义应用的时延、抖动和丢包的阈值，转发面实时监测每条链路的时延、抖动和丢包指标，并根据应用的SLA要求，当应用当前流量路径质量劣化到阈值以下时，系统自动将应用调度到满足SLA约束的链路上。

ANP目前支持的应用识别规则包括目的IP地址段、协议+端口、域名、正则表达式等四种方式，分别如下处理逻辑：

- 域名规则，ANPOS 控制面通过解析客户端的 DNS Response 来匹配域名规则，并取出 DNS 中的 A/AAAA Record IP 地址信息，下发到转发面。对于域名匹配，系统支持基于后缀的长匹配规则，比如 a.com 可以匹配所有的*.a.com 的子域名，但如果明确配置了 x.a.com 的规则，那么其优先级要高于通配的 a.com 域名规则。
- 正则表达式规则：X86 架构设备开启 DPI 引擎，可以对常用的协议大类进行特征匹配，如 HTTP/HTTPS、QUIC；针对具体的协议大类，用户可以设置对应的正则规则进行 DPI 应用识别，识别结果标记为一个应用分类，复用系统框架中的应用策略；基于正则表达式的策略优先级在四种策略匹配中优先级最低。

4.9 创新的控制面和转发面配置对账技术

分布式系统中数据的一致性是个难题，尤其是对于SD-WAN这样的管理通道不稳定的广域网系统，问题更加突出。传统领先厂商的SDN系统均实现了较为简单的配置对账功能，也就是周期性把配置数据全部读取到控制器上进行对比，这个方式极其消耗时间和带宽，对于成千上万的SD-WAN系统以及CPU较弱的CPE系统而言，这个方法难以实际实施。易科腾通过引入将类似于Merkle树的对账机制引

入到系统中来，对每个数据记录原生设计携带UUID和更新的时间戳，对这两个字段的Hash构建完整的Merkle树。最终可以支持无论多少条记录，纠正错误的配置数据可以在秒级完成。

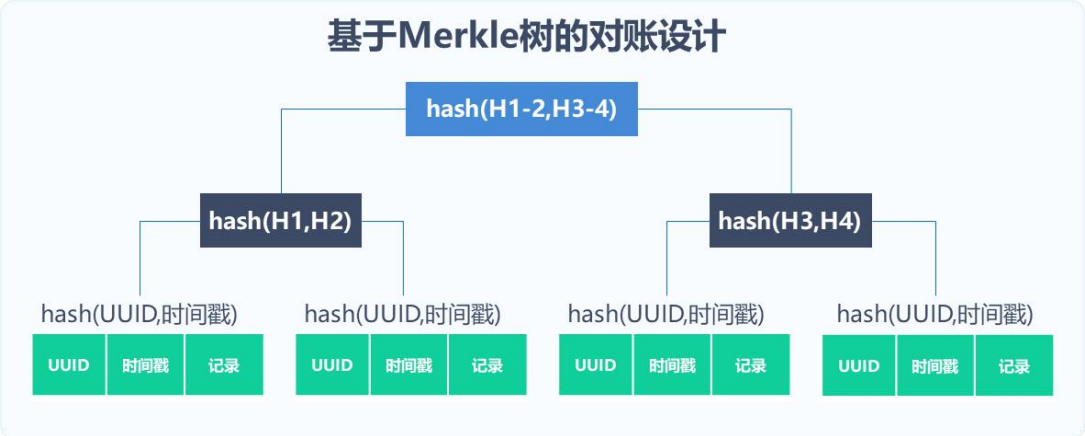


图 4.2

4.10 广域网大二层支持

易科腾ANP系统转发面采用VXLAN或VXLAN Over IPSec封装形式，支持跨地域的大二层组网，支持同一个租户下二层和三层混合组网。

为了降低大二层组网时的广播风暴问题，ANP系统支持Anycast网关，对ARP进行代答，避免ARP广播穿越广域网。

4.11 支持 NAT 出口企业网的动态路由接入

如果客户站点网络规模较大，则需要和CPE通告动态路由协议，并且SD-WAN系统也必须将每个站点的动态路由通告到同租户下的其它站点，在专线组网的情况下，部分厂商采用了部署BGP/EVPN RR(Route Reflector，路由反射器)的方式，需要CPE和RR通告路由，这种方式的缺陷非常明显：

1） BGP协议不支持穿越NAT，如果客户站点不是专线，也没有公网IP地址，则此方案不可行。

2） RR方案支持的网络规模非常有限，一般就在几百的节点，并且对于CPE这样的低端设备，RR的路由通告不区分租户/VRF进行全反射，在不稳定的广域网下是否能够正常运行都是问题

易科腾ANP解决方案通过CPE和控制器之间的gRPC通道通告路由，即使CPE没有公网地址也可以

正常进行路由通告。同时控制器维护虚拟拓扑，将路由只通告到同一个虚拟拓扑(一个VRF)下的相关CPE设备上，大大减少了控制面的负担。进一步地，ANP还采取了延迟撤销路由等技术，使得动态路由即使在超大规模组网、不稳定的广域网上也可以稳定商用。

4.12 广域网优化技术

SD-WAN作为一种广域网互联方案，除了基本的虚拟专用网络、加密传输以及智能自组织外，也内置和安全和网络优化的功能，其中广域网优化技术包含了一系列优化手段用于提升客户的网络体验。包括如下技术：

- 丢包自动重传ARQ
- FEC前向纠错
- 双发选收
- 报文压缩

丢包自动重传ARQ：报文重传可以显著降低末端可以感受的丢包率，采用一次丢包重传，丢包率可以降低到原来丢包率的平方，例如将10%丢包率降低到1%，两次重传则为立方关系，网络设备提供报文重传能力的价值在于网络设备的逐跳时延远远小于业务端到端的时延，从而可以在实时业务场景中通过重传弥补丢包并且不损失业务体验。

双发选收：ANP SD-WAN支持双LTE、双5G链路、固网接入+LTE/5G等多种接入方式的双发选收。通过在客户网络侧部署CPE、网络中设置1个或多个汇聚网关实现完整的双发选收的优化。对于配置了双发选收功能的逻辑链路组，CPE和网关之间建立两条加密隧道构成逻辑链路组，CPE和网关之间的这对链路组均对指定的报文进行双发选收。发送方将客户的报文复制在两条逻辑链路上，接收侧进行报文的去重处理，仅仅转发一份报文。

FEC功能：网络层面的FEC目标是为了抗丢包，而不是进行报文bit的纠检错，因此是采用的帧间编码，通过计算一组报文的校验和获得FEC，后期丢失某个或者某几个报文可以通过FEC恢复。

报文压缩：目前选取了gzip和deflate压缩算法， 压缩开销比较大，在ARM设备上CPU算力有限，启用压缩后，无丢包吞吐下降30%以上，而在x86机器上，CPU不是瓶颈，表现更好。由于当前网络

的大部分流量是加密报文或者视频流，难以压缩，故而对报文进行了初步判断，如果是加密报文或者压缩后受益不大的报文就采用原始报文进行传送，以免浪费CPU时间。

4.13 全面 5G 特性支持

ASG全系列产品采用符合3GPP R16规范的模组，全面支持5G切片、多APN、5G LAN功能，支持双5G CPE，并可以基于双5G进行流量的负载均衡和双发选收

4.14 微分段安全

ANP微分段安全和AWS、OpenStack的安全组机制类似，支持租户定义多个安全组，每个安全组可以配置一组安全策略，简单地将安全组成员加入到安全组，ANP系统就可以自动查找安全组成员所在的位置，并下发安全过滤策略到指定的CPE或中心站点。安全组规则默认是白名单机制的有状态防火墙规则。

支持的安全组成员类型包括两种：CPE设备、IP地址段、客户端账号，后一种情况用于控制同一个分支下不同主机、部门的不同网络访问权限。

4.15 智能 DNS 代理

系统可根据特定域名进行代理/重定向至指定DNS服务器进行域名解析，可基于应用设置不同的DNS服务器，并可以结合应用分类进行灵活的路径选择

4.18 端到端加密技术

全系CPE支持端到端加密隧道，可以实现跨POP组网场景下的端到端数据加密，保证中间结点无加解密，用户数据不落地，满足高等级数据安全；端到端加密隧道基于控制器自动化编排框架，可以实现一键配置下发以及密钥的周期性安全更新。

5. 标准应用场景

5.1 标准的企业分支组网

无论是普通的企业分支组网、工厂互联、门店互联，都可以归属到本类下，区别是不同场景、不同站点的流量大小、成本约束不同，需要选择不同规格的硬件设备。

- 如果企业区域相对集中，可以采用私有的POP进行汇聚。如果企业有私有云资源，可以将基于ASG2000v的POP部署在私有云中，采用标准的CPE+POP的Hub-Spoke方式组网；如果企业没有私有云，也可以在总部部署硬件CPE作为流量的汇聚点，CPE接入到
- 如果企业是全球化组网，可以在公有云或租用IDC资源部署POP点，分支机构就近入网，POP点间Full-Mesh组网，进行不同区域之间的流量中转。

在企业分支组网场景下可以充分利用ANP的微分段安全能力做好分支总部的安全防护，同时可以启用基于应用识别的上网行为管理功能，控制分支机构对Internet、核心业务系统的访问权限，并保证带宽用于承载企业的核心应用。

5.2 SD-WAN 专业运营商组网

- 无骨干网方式，运营商可以租用公有云或者IDC资源作为POP，POP之间可以按租户虚拟拓扑配置POP间VXLAN隧道，处理区域间中转流量，构建一个虚拟骨干网。每个POP都可以为最多4000个租户共享，每个租户都可以配置相应的配额。
- 有骨干网方式，采用ANP ASG2000/2000v建设POP点，汇聚就近CPE，同时POP设备和骨干网的连接有两种方式：
  - ✓ 精细化VPN组网，SD-WAN POP和PE以BGP OptionA的方式组网，将每个租户的VRF映射到VLAN子接口，在PE上进入相应的骨干网MPLS VPN。此方案的好处是骨干网可以看到每个SD-WAN租户，可以做精细化带宽和流量工程。缺点是开通复杂、骨干网需要对接的信息也过多。
  - ✓ 骨干网作为Overlay方式。SD-WAN POP点就近接入骨干网，但是POP点间直接建立VXLAN隧道，无需将租户信息和骨干网VPN进行映射。如果需要QoS保证，POP设备应将相应的租

户的VXLAN外层打上不同等级的DSCP标签，骨干网信任DSCP，并匹配DSCP标签进入相应的MPLS TE隧道。

5.3 企业远程办公场景

可以在标准的企业分支组网或SD-WAN运营的基础上叠加企业远程办公。在ANP的体系架构下，任何一个POP点，或总部CPE设备都可以作为远程办公的接入点。在控制器上为特定的租户配置启用远程办公，则控制器会在租户对应的服务节点(POP和总部CPE节点)上使能远程办公功能，同时需要创建远程办公的帐号密码、导入客户端软件的证书。客户下载客户端软件并安装激活后就可以拨号接入企业的私网。

5.4 企业入云和多云互联场景

易科腾 ANP 系统中的 ASG2000v 支持公有云部署，目前也已经适配主流的公有云平台。企业可以将 ASG2000v 当作 vCPE 以虚机方式部署在公有云的企业 VPC 中，而无需租用公有云的 VPNaaS 服务。

在 ANP 系统中，受 ANPC 控制的 vCPE 可以像 CPE 一样自动连接到 POP 汇聚设备，如果企业在多个云上租户了 VPC 资源，则可以统一规划私网地址，通过 ANP 的 vCPE 将多个云的 VPC 连接到企业的 SD-WAN 汇聚 POP 设备上，从而实现了局域网内一样的访问体验。

如果希望云端的应用一样能够主动访问企业的内网应用，则需要在公有云的 VPC 中注入企业私网的明细路由，并将其下一跳地址指向 vCPE 的接入端口 IP 地址。如果无需互访，则启用 vCPE 的 LAN 口 (连接 VPC 内网接口) 的 SNAT 功能，这样只允许企业访问云 VPC 资源，而不能反向访问。

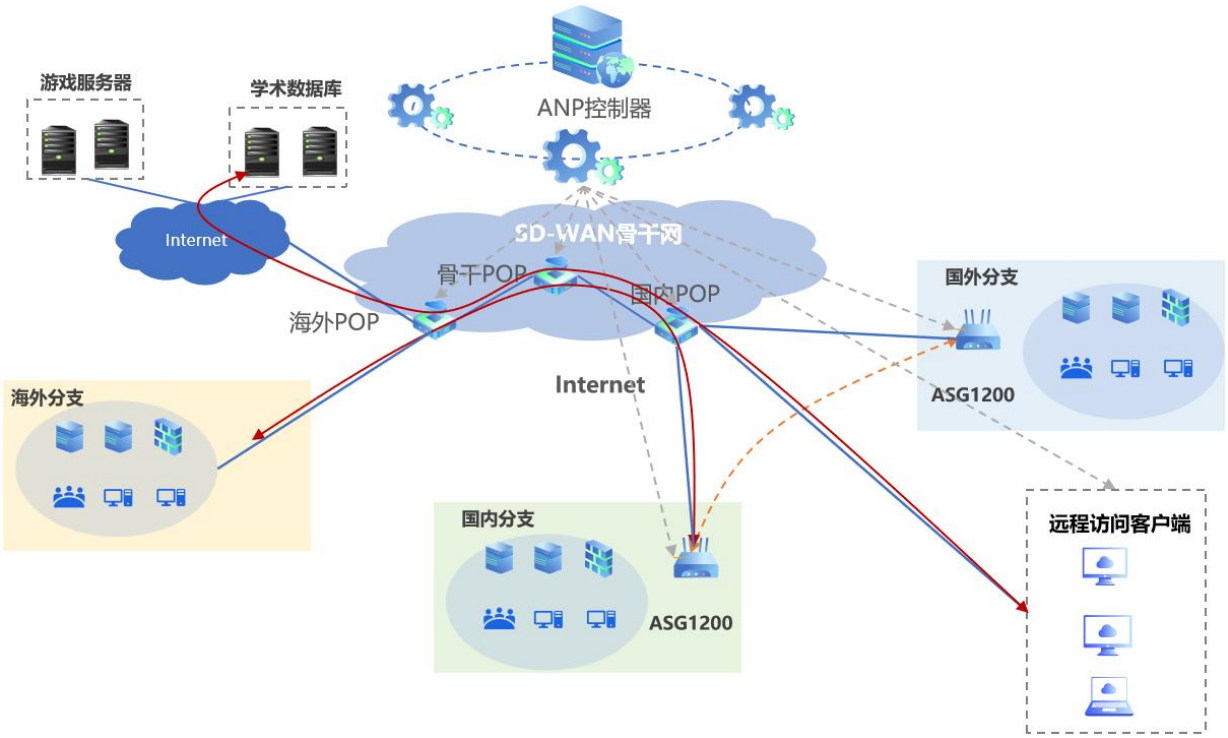
5.5 跨境加速场景

国内外分支、远程接入用户就近接入SD-WAN骨干网络，通过骨干网动态链路质量测量结果，实

时选择最优路径。基于DPI/DNS域名/五元组结合实现应用识别；数千种应用识别库，控制器定期更新应用规则。可以基于应用SLA阈值的应用选路，基于链路质量的自动化切换，保证关键业务连续性和优质体验。设备内置国内外数百高校、上千款游戏应用识别库，基于应用类别按需开启，真正的一键链接，全球加速。

此外ANP系统提供多租户共享接入，用丰富的SD-WAN POP节点构建优质骨干网络，基于用户签约带宽保证，多租户VPN网络安全隔离。

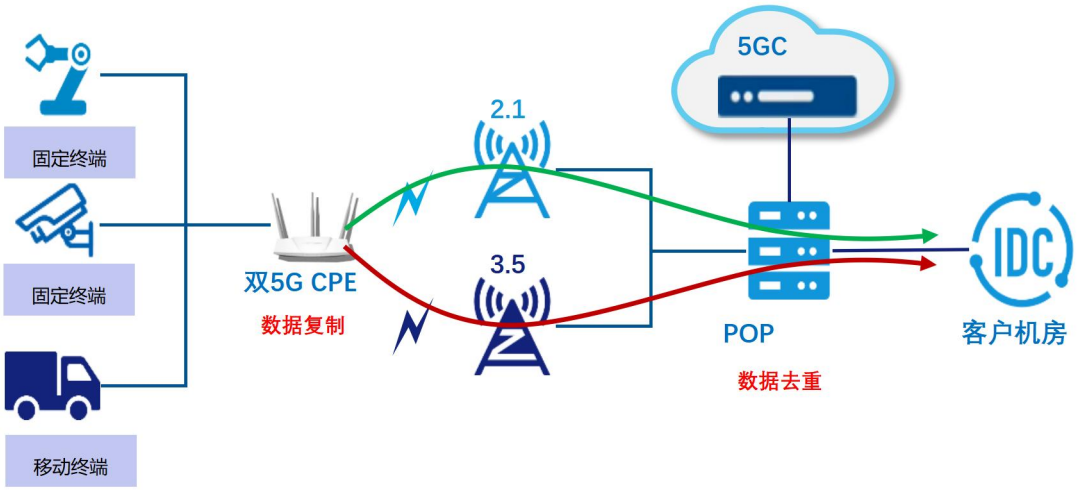
集中化管控平台，应用加速结果可视化，效果看得见。并提供PC/MAC/IOS/Android等移动端产品，基于账户提供精细化业务加速，体验有保障。



5.6 5G 工业控制组网

工业场景解决方案，在保障设备稳定性、易用性的同时，提供高可用低时延的数据传输，将控制/业务/视频数据传输至总部集中管理。工业控制及相应配套的PLC设备通过5G/有线CPE双发选收能力提供高质量无线有线数据传输；硬件设备提供远程管理、远程运维功能，降低人力成本通过创建虚拟专用网络，将各数据统一上传至总部监控中心工业化设计，适应复杂环境云端管理，降低维护成本；

链路加密，数据传输安全。



价值如下：

- 双网智能切换：SD-WAN设备实现原有有线网与5G网络快速切换。3.5G+2.1G双频组网，控制信号、视频信号等多类数据分频分路、差异化QoS策略传输；
- 智能运维：统一管控平台，支持远程对现场设备进行在线可视化管理，网络流量信息、无线链路质量实时可管、可视；提供应用的流量和业务质量报表，关键业务传输有保障；
- 高可靠性：在中心端（专用5G小型核心网）、防火墙双机部署中心端切换单元（SD-WAN）、双5G CPE远端都实现双热备冗余，保证不出现单点故障导致业务中断；
- 网络优化：重型机械关键操作数据的双终端冗余传输，将5G空口丢包率降至万分之一的水平。

设备实现双发选收，支持无线与核心网异厂家组网场景

5.7 物联网互联场景

5.7.1分布式风光电站

风光伏电站一般遍布多个地区，海量站点设备需要统一管理；同时不同区域光伏电站资产管理权限需要严格区分，实现区域——总部的分级权限控制；易科腾SD-WAN内生多租户运营级架构，一套系统可以管理上万台设备，真正实现全国甚至全球光伏电站网络的统一管理，实现网络资源的运营平台。

光伏电站有地处滩涂、沙漠等偏远地区，网络线路覆盖差，现场作业条件艰苦；易科腾SD-WAN CPE设备可提供有线/4G/5G等多种接入链路，充分利用光伏电站现场线路资源，提供多链路冗余保护，减少网络改造成本和周期；易科腾SD-WAN设备实现零配置部署开局，现场仅需将设备上电、连接网线，无需现场进行邮件或U盘开局配置，其他所有业务均可远程开通，降低现场人员要求和作业难度，极大提高站点业务开通效率；同时设备采用All in one架构，单台设备就可提供路由、VPN、应用识别、防火墙、网络优化的全量功能，降低对于光伏电站机房空间、布线要求，降低系统维护成本。

光伏电站网络线路资源差异性大，部分站点无专线网络覆盖，甚至没有有线网络覆盖。易科腾SD-WAN通过灵活的组网设计，利用现网资源，极大降低网络线路改造成本：站点没有固定公网IP的专线或互联网专线，设备可通过PPPoE获取的动态公网IP，甚至是1：1 NAT之后的公网IP实现组网，作为hub节点，汇聚区域内光伏电站监控流量，降低部署专线的网络建设成本；易科腾提供公有云或者私有云部署的软件vPOP，多租户共享，无需每个用户分配单独的公网IP，减少公网IP购买费用。

光伏电站系统太阳能发电系统运行状态，发电效率等关键业务数据需要实时准确呈现，辅助电站扩容或者选址决策；同时基于实时数据判断系统故障，辅助光伏系统故障定位。易科腾SD-WAN提供可视化运维页面，设备运行状态，链路质量（延迟、抖动、丢包）、应用流量实时呈现，秒级刷新，提供超长历史数据查询，电站网络流量可视化；通过自定义的流量报表，提供详实的系统运行状态报告；提供网络链路状态、流量阈值、设备运行状态的异常告警，提供详细的业务描述和恢复手段导引，帮助客户智能排障；

针对光伏电站联网数据的安全传输要求，易科腾提供端到端的数据传输加密，支持国密算法；终端设备基于数字证书认证方可接入系统，支持设备系统安全加固，远程禁用/启用设备，可以实时保障系统风险最小化；设备通过安全组+IPS可以精细化对业务访问和流量行为进行精细化管控，实现零信任网络模型，按需授权，全方位保障网络安全。

5.7.2智能停车场

随着汽车保有量的激增，城市普遍存在“停车难“的问题，急需采用现代化手段对停车场实行高效智能化管理，大力发展智慧停车场数字化运营，以满足停车场适应快节奏的车辆进出。如何将分布在停车场各处的电子设备建立高速稳定的无线网络连接，就成为了实现智慧停车场数字化运营的关键。

业务开通：无需架线，快速布网，随时随地便捷网络接入；摄像头、道闸一体机、控制机等无需改造即可无缝接入；现场网络策略自动下发，无需复杂的网络调试，实现分钟级业务上线。

可靠性： CPE采用无线方式接入，接入双POP，故障自动切换；对于大型停车场，可选用双4G/5G CPE，提供双无线通道；支持WAN优化技术，基于双发选收、丢包重传优化无线传输质量。为进一步提升网络可靠性，可以选择在公有云部署一对或者多对POP，可以服务于上千台CPE的统一接入。

智能化运维：统一管控平台，支持远程对现场设备进行在线可视化管理，网络流量信息、无线链路质量实时可管、可视化；可以直接通过IP地址访问任意停车场的闸口设备、摄像头，极大地简化了设备维护方式，降低故障修复时间。

安全性：数据全程端到端加密，多POP网络备份；SD-WAN设备双重认证接入，设备防盗用；零信任访问授权、有状态防火墙隔离各个停车场的监控和业务数据。

5.7.3充电桩

新能源汽车行业快速发展过程中衍生出充换电的需求，充电桩行业在前期受大量的政策与补贴驱动，加快建设进程，近年来车桩比维持在3:1上 下。伴随着充电桩市场格局逐渐稳定，厂商盈利模式日渐成熟，充电桩建设也在由补贴驱动逐渐转向市场驱动。在充电桩数量急剧暴增的情况下，保证充电桩安全管控，业务数据通信稳定高效传输，成为迫切需要改善和解决的问题。

部分充电桩受限于物理环境，不具备有线接入互联网条件，增加了充电桩网络接入的难度。易科腾CPE支持4G/5G无线接入方式，无需架线，快速布网，随时随地便捷网络接入。

充电桩每个区域各运营商网络环境不一致，郊区、地下室等，通信信号差，网络连接不稳定。易科腾CPE支持采用WoC网络优化技术，采用双发选收、自动丢包重传等，保证充电桩业务数据和总部控制监控平台高效率通信，有效改善网络质量。并且CPE安全可控，内置轻量级防火墙、双链路冗余机制，保障充电桩数据传输的安全性和可靠性。

现有停车场为传统广域网组网方案，无法统一远程管理摄像头、停车场控制机等设备，需要人员现场巡检。易科腾CPE支持远程对现场设备进行在线管理，支持停车场多个充电桩IP地址重叠访问；远程运维，网络运维一体化，可视、可管、可控。