RTT 技术白皮书

APPEX NETWORKS

目　录

RTT (Real-Time TCP Tunnel，实时 TCP 隧道) 是由北京华夏创新科技有限公司（简称：华夏创新）自主研发的一种隧道传输技术，华夏创新将该隧道应用于其覆盖全球的自运营 SD-WAN 网络服务平台 CloudWAN 中，作为该平台的 SD-WAN Overlay 隧道承载其所服务的企业客户的办公应用流量。

一、为什么要自研 RTT 隧道技术

业界多数 SD-WAN 产品通常都是采用 IPSec、SSL、GRE 或者 VxLAN 等传统隧道技术作为 SD-WAN Overlay 传输隧道，而华夏创新则选择了自研专用的 SD-WAN Overlay 隧道技术，其原因主要有如下几点。

1. 获取极致的网络传输效率

一般情况下，网络数据传输效率越高，则上层应用的响应效率和体验越好。在面向远距传输、尤其是跨境传输场景时，传统 IPSec 等隧道技术往往存在传输效率低下、不稳定等问题，导致用户使用体验不佳。为了在各种复杂网络环境下都能够向企业客户提供最佳的传输质量，华夏创新舍弃了传统隧道技术，选择自研融合了 ZetaTCP® 广域网优化专利技术和多发选收优化技术、具备极致传输效率的 RTT 隧道。

2. 实现真正的全球网络覆盖

建设覆盖全球的 SD-WAN 骨干网，需要综合考量可选链路资源、链路质量与带宽成本间的平衡。一般情况下，发达区域可选的专线链路资源较多、质量较高，且同时带宽成本较低；而欠发达区域则往往可选的链路资源较少、高质量的专线链路资源更少，追求高质量专线链路就意味着极高的带宽成本投入，而这些

成本投入最终必然会转化为企业客户使用 SD-WAN 服务时所要付出的成本；某些极度欠发达区域甚至完全没有高质量的专线链路资源可用，在这些区域如何为企业客户提供满足质量要求的 SD-WAN 骨干网接入服务就成了一个难题。

具备极致传输能力的 RTT 隧道则是华夏创新解决这些问题的取胜之匙。对于无高质量专线链路或者高质量链路成本极高的欠发达区域，RTT 隧道的极致传输能力使华夏创新能够使用中低质量、中低成本的专线或者互联网链路建设骨干网，同时又能够满足企业应用正常使用的传输质量要求。在一些完全不具备有线链路接入条件的使用场景下，华夏创新甚至可以通过移动无线链路、卫星链路等资源提供满足基本使用要求的骨干网接入服务。

RTT 的传输能力让华夏创新实现了真正意义上的全球网络覆盖。

3. 保障数据传输的安全性

基于成本、效率及灵活性等方面的综合考量，企业客户使用 SD-WAN 骨干网络服务时，一般是使用其办公站点现有的互联网链路通过加密隧道技术接入 SD-WAN 骨干网络。如果企业办公站点使用传统 IPSec 等隧道技术接入 SD-WAN 骨干网络，则往往需要在抵达 SD-WAN 骨干网络的 PoP 节点时对 IPSec 隧道进行解密，以便其内部封装的用户流量能够在 PoP 节点上进行路由匹配从而确定下一跳路径。在确定下一跳路径后，用户流量则会重新进入下一跳隧道；当用户流量需要流经多个 PoP 节点才能抵达目的地时，这种“解密-再加密”的操作就会多次发生。（注：某些服务商的方案中，如果路径上两个骨干网 PoP 节点之间使用专线资源进行互联的话，用户流量会直接以明文的形式经专线路径去往下一跳 PoP 节点）。而这种“解密-再加密”的操作，极度加剧了企业在使用 SD-WAN 骨干网络服务时其重要业务数据被泄露及篡改的风险。

为了消除这种风险，彻底保障企业数据传输过程中的安全性，华夏创新在自研的 RTT 隧道中实现了“端到端加密”技术：RTT 隧道内的企业用户流量在部署于企业办公站点内网的 CloudWAN CPE 设备上面完成加密，其后在流经路径上的任意 CloudWAN POP 节点时都不再需要解密，直到其抵达部署于目的端企业办公站点内网的 CloudWAN CPE 设备时才会进行解密。

4. 实现应用不中断的路径平滑切换

企业客户流量流经 SD-WAN 骨干网时，某些情况下会遇到路径上某个 PoP 节点负载变高或者异常故障宕机等问题，此时一般会基于 SD-WAN 的智能路径切换功能将企业流量切换至其它可用的 PoP 节点以确保企业办公业务能够继续正常使用。但是在切换发生的极短时间内，基于传统 IPSec 等隧道技术的 SD-WAN 方案往往会导致当前流量中断一下，而这种“中断一下”则往往又会导致用户业务（如视频会议）的中断，从而影响用户的使用体验。

认识到传统隧道技术的这种不足，华夏创新在自研 RTT 隧道技术中实现了无缝平滑切换的能力，确保在出现传输路径切换时用户流量不中断、用户业务无感知。

5. 保障跨平台的可移植性

一般企业办公场景中，除了办公站点中通过部署 CloudWAN CPE 设备来使用 CloudWAN 的服务之外，在移动办公场景中还要支持用户通过在电脑、手机及平板等各类智能终端上面安装软件客户端来使用 CloudWAN 的服务，在企业上云场景中则还要支持用户通过在云中部署虚拟化 CPE 设备（vCPE）使用 CloudWAN 的服务。

另外，除企业办公场景外， CloudWAN 的系统设计同时考虑了对工业互联

网、工业物联网应用场景的支持。而在工业互联网、工业物联网应用场景中，CPE、vCPE 及软件客户端往往都无法适用，需要通过嵌入式软件部署的方式来使用 CloudWAN 服务。

以上这些不同类型的应用场景，对 CloudWAN 在终端侧的部署能力提出了极高适配性及灵活性的要求。如果使用传统 IPSec 等隧道技术，即使不考虑 CloudWAN 其它功能所依赖的软件模块，仅就隧道相关的功能模块而言，其对终端系统中各类资源的要求就难以灵活适配如此多的应用场景。而华夏创新自研的 RTT 隧道技术则从设计之初就充分考虑对各类终端环境、尤其是低资源终端环境的适配性，从而可灵活部署于各类应用场景中。

二、RTT 的传输优化能力

RTT 主要通过协议优化和多发选收两项技术对其网络传输能力进行保障。

1. 协议优化

RTT 融合了 ZetaTCP® 广域网优化专利技术。ZetaTCP® 是基于智能学习算法（Learning-based）的 TCP 加速技术，采用网络路径特征自学习的动态算法，基于每一个 TCP 连接实时观察、分析网络特征，并根据学习到的网络特征随时调整算法来更准确地判断拥塞程度、更及时地判断丢包，从而更恰当地进行拥塞处理并更快速地进行丢包恢复。智能学习算法从原理上克服了静态算法无法适应网络路径特征变化的问题，保证了在各种不同网络环境下、面向各种频繁变化的网络延迟、丢包特征时加速效果的持续有效性。更多关于 ZetaTCP® 优化技术的详细介绍请参见《ZetaTCP®技术白皮书》。

华夏创新将 ZetaTCP® 优化技术融合应用于 RTT 隧道中，使 RTT 隧道具备了在全球各种复杂网络环境下的高效传输能力，从而确保企业应用业务数据经 RTT 隧道传输时的及时性，确保企业全球办公的效率和体验。

2. 多发选收

在 ZetaTCP® 优化技术的基础上，华夏创新进一步研发了“多发选收”传输优化技术，将 RTT 对企业应用流量的传输保障提升到极致。

“多发选收”技术在发送端将一份网络封包复制为多份完全相同的网络封包，并将这些封包分别经多条不同路径的 RTT 隧道同时发送出去；接收端只要收到多份网络封包中的任意一份就可视为传输成功，后续抵达的其余复制封包则会被接收端丢弃（接收端通过网络封包的序列号来确认当前抵达的网络封包是否为某个已接收过的网络封包的复制包）。

“多发选收”技术可为企业关键应用提供更进一步的传输保障，确保关键应用不会因网络传输路径中的某一段甚至整条网络路径出现故障而中断。由于“多发选收”对同一网络封包进行复制传输，会消耗额外的网络带宽资源，因此一般只针对关键应用启用“多发选收”进行传输保障。

三、RTT 的传输安全性

RTT 隧道通过“端到端加密”技术确保企业应用数据传输过程中的安全性。

一般情况下，在使用 SD-WAN 骨干网进行传输路径优化时，基于传统 IPSec 等隧道技术实现的 SD-WAN 方案只能采用“分段式加密”方式对企业应用数据进行加密传输。“分段式加密”在途径的每个 PoP 节点上面都要对企业应用数

据进行“解密-再加密”操作，导致企业应用数据面临被泄露和篡改的风险。

相对于“分段式加密”，华夏创新的 RTT 隧道技术则采用“端到端加密”方式对企业应用数据进行加密传输。在“端到端加密”模式下，企业应用数据在位于发送端办公站点内网的 CPE 设备上面完成加密，直到抵达位于接收端办公站点内网的 CPE 设备上才会进行解密，而在途径的任意 PoP 节点上都不会进行解密操作。

为实现“端到端加密”，RTT 隧道采用了双层封装的隧道设计。其外层封装用于实现 Overlay 路径搭建，基于“标签交换”（Label Switching）技术实现在路径上逐跳 PoP 节点间的网络封包转发；内层封装则用于“端到端”数据加密。在途径某个 PoP 节点时，PoP 节点只对外层封装的包头进行解析，获取其下一跳 PoP 节点的相关信息之后，将外层封装包头中的目的 IP 字段修改为下一跳 PoP 节点的 IP 地址，然后进行转发；PoP 节点完全不触碰内层封装（由于加密密钥是由两端 CPE 设备协商创建的，因此 PoP 节点本身也不具备解析内层封装加密的能力），从而确保企业应用数据经 RTT 传输时的安全性。

四、RTT 的路径平滑切换

为了向企业客户提供最优质的 SD-WAN 骨干网传输质量，某些情况下（如路径上某个 PoP 节点满载或故障、当前路径不再满足 SLA 要求，等等）需要进行实时的骨干网路径切换操作（注：实时路径切换一般是由 CloudWAN Orchestrator 基于对全网实时监测的结果自动下发操作指令来完成的）。

而为了保障企业应用不会因路径切换操作出现业务中断、确保企业应用对路

径切换无感知，RTT 实现了路径平滑切换功能。

路径平滑切换是在 RTT 双层隧道封装的基础上得以实现的。在具体实现方式上，RTT 的外层隧道是由逐跳路径上的一段段隧道拼接而成的，RTT 的内层隧道则是以外层隧道为承载而建立起的“端到端”隧道（注：“端到端”是指从一端 CPE 到另一端 CPE），企业应用的流量则是流通于内层隧道之中。发生路径切换时，外层隧道基于最新的路径指令进行新的逐段隧道拼接以完成路径切换；而内层隧道则对路径切换无感知，只要起点和终点两个端点不变，内层隧道就可以认为是无变化的。而在内层隧道保持不变的情况下，流通于内层隧道中的企业应用流量就完全不受外层路径切换的影响，从而实现了路径平滑切换。可以把外层隧道、内层隧道和企业应用流量以具像化的方式类比为铁轨、火车和乘客：铁轨通过道岔变轨完成路径切换，火车则对道岔变轨操作完全无感知，只要始发站和终点站不变，火车车次就保持不变，而坐在车厢内的乘客就更感知不到铁轨路径的变化。

五、RTT 的可移植性

RTT 采用极为轻量化同时又极具弹性的设计实现，既可运行在拥有超多核高频处理器、上百 GB 内存空间、单台可处理 40 Gbps 流量吞吐的高端工控机硬件平台上，也可运行在只有低频处理器、几兆内存空间的物联网终端上。良好的轻量化弹性设计使 RTT 目前已成功移植到各种不同的系统平台，包括 x86 架构的工控机、虚拟化云主机、MIPS/ARM 架构的路由器或摄像头、车载设备、物联网设备、各类手持智能终端等等，从而可以满足各种不同使用场景的需要。

北京华夏创新科技有限公司

地址：北京市海淀区北清路 68 号院 24 号楼 C 座 6 层 601 室

网址：https://www.appexnetworks.com.cn/

邮箱：marketing@appexnetworks.com

中国大陆区域：400-606-6118

北美区域：888-473-1388

韩国区域：003-0864-0156

其他区域：0086-29-81157308