厚积薄发

---------新一代网络操作系统 VRP V8

文/许义国

导语

近年来，由苹果 iPhone 智能手机携 App Store 应用所刮起的移动互联网风潮席卷全球,移动宽带流量呈现井喷增长;由 Google,亚马逊等互联网厂商所开创的云计算模式对原有计算/存储/网络资源的利用方式带来了巨大的冲击,传统数据中心的变革拉开序幕. 不管是移动互联网,还是云计算,业务的增长和商业模式的变革都驱动着底层物理设备架构需要与之相适应.而作为承载业务并确保用户应用体验重要管道的网络设备,它的灵魂-------网络操作系统则肩负着革新的重大使命.

我们可以看到,这个使命不是在目前的操作系统基础上简单修改升级，增加几个新协议、新特性可以解决，而必须要在架构层面做出更深层次的考量与改变，由传统的网络操作系统跨向新一代的网络操作系统。

新一代网络操作系统具有怎样的身手？能为我们带来怎样的惊喜呢？华为携 15 年网络操作系统的研发商用积累和 500 项技术专利,与我们一道来揭开它的神秘面纱,一起细细品位”厚积薄发”的华为新一代网络操作系统 VRP V8.

1 应运而生

IP 技术起源于上世纪 60 年代美国军方的内部研究和应用.它强调极高的时效性和可靠性,即网络必须经受得住故障的考验而维持正常的工作，一旦发生战争，当网络的某一部分因遭受攻击而失去工作能力时，网络的其它部分应能维持正常的通信工作。

凭借其开放性和简单性，IP 技术得到民用,迅速发展成为通信网络的基础设施。直至今天，IP 技术组建的网络支撑着语音、数据、视频、电子商务、游戏等各种多媒体应用,潜移默化地改变着人类的生活。人们越来越依赖由 IP 技术构建的全球互联网。构成这个全球互联网的最基础的单元通常是路由器和交换机，也就是我们所描述的 IP 网络设备。

伴随着近二十多年来 IP 网络设备技术的革新、规模的扩展和应用的普及,运行在其上的网络操作系统也在整个网络业务和应用的推动下不断完善和发展，在其二十多年的发展过程

中经历了三次大的革新。

1.1 第一代 IP 设备操作系统_单进程

第一代 IP 设备操作系统，是为早期的 IP 设备设计。由于当时受硬件条件限制，此类操作系统的典型特征是基于单进程的系统，提供比较有限的系统可靠性。系统实时性保证相对困难，业务容量小，操作维护方面考虑相对较少。对于第一代操作系统,任何的修改和扩展由于其紧耦合、单进程架构，都需要大量人力进行测试验证；系统因为单进程架构无法进行很好地故障隔离，只要一个 BUG 就崩溃重启导致业务中断。

1.2 第二代 IP 设备操作系统_多进程

第二代 IP 设备操作系统随着业务发展需求和实时业务要求，采用了多进程、有限的分布式架构，实现了更好的可靠性。它采用多进程的数据共享方式设计。该类系统虽然比以前有了加大改进，但是由于共享设计同时要兼顾实时性，必然要大量的互斥操作，稍有不慎就会导致系统死锁。另外第 2 代 OS 没有实现真正电信级可靠性，无法做到不间断路由服务. 这在数据中心以及云计算网络尤为突出。用户需要有更长的设备持续运行时间，并期望将网络升级对业务的冲击降至最小甚至没有影响.

1.3 第三代 IP 设备操作系统_虚拟化

第三代操作系统采用了多进程、分布式和虚拟化的架构,具有如下特点:

1) 顺应了CPU的发展趋势,即从单核到多核的发展方向。多核通过集成更多的CPU内核提高计算能力。这些都要求操作系统具备细粒度多进程机制，以充分发挥这些多核CPU的计算能力来满足不断攀升的大容量实时业务的计算要求。
2) 新一代网络操作系统采用了完全的模块化结构，各模块运行空间隔离，单个模块的异常不会影响系统其他部分，提高了系统的可靠性
3) 提供了在无需其它设备协助的情况下，做到不间断服务的能力.
4) 具备了良好的运营维护能力，降低用户使用过程中的成本。

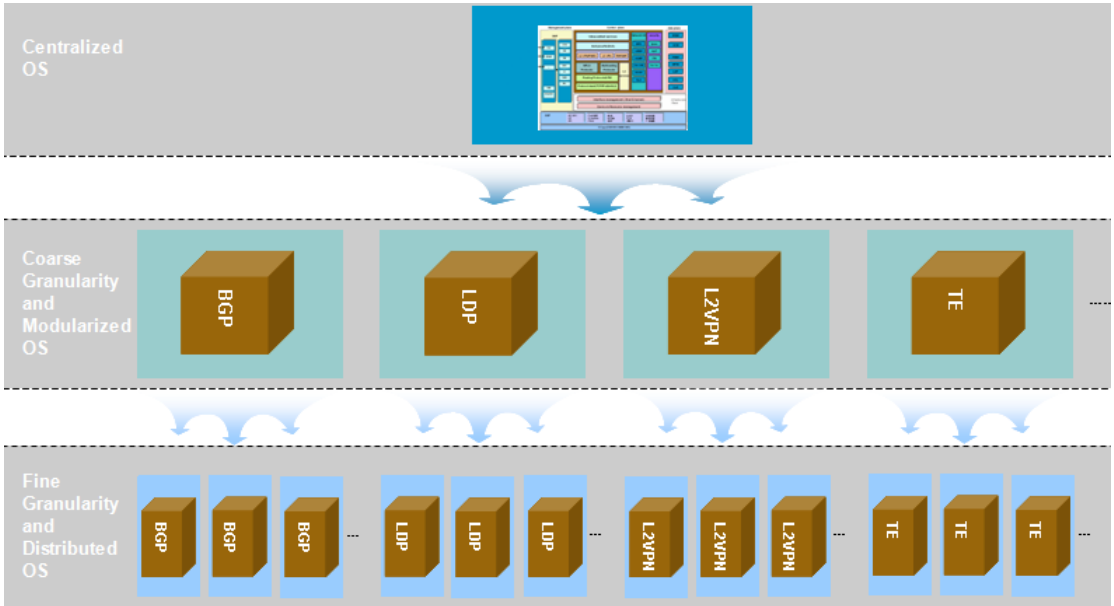
华为 VRP V8 平台顺应了网络应用的发展趋势，特别呼应了数据中心和云计算网络的发展需求,在高性能、虚拟化、特性丰富度、电信级可靠性等方面都进行了深度的考虑和设计,是当前第 3 代 IP 设备操作系统的典型代表.

2 新一代网络操作系统的特点

2.1 面向未来的高性能和高扩展性

随着网络规模和业务量的增长，特别是超大数据中心的建设，网络层设备面临越来越大的处理能力和性能压力。老一代操作系统虽然采取多进程工作模式，不同的协议可以独立运行，性能和容量有了一定的可扩展性. 但由于不支持单个协议的分布式运行，仍不能充分发挥硬件多核的优势，充分提高性能和容量.

华为新一代操作系统 VRP V8 采用了全业务细粒度分布式架构，对性能和容量有要求的协议/业务组件可以多实例分布式并行处理，突破硬件单核处理能力及单 CPU 内存空间的限制,通过软件充分利用多 CPU 的能力，使得原来被闲置的 CPU 都参与到系统的运行中来,以便达成系统能力的最大化，提升性能和容量.VRP V8 根据不同协议处理的并行度特点设计了灵活的分布式策略，比如 BGP 基于 Peer 分布、LDP 基于 Session 分布，L2VPN 基于业务实例分布，TE 基于接口组分布等等。VRP V8 的细粒度分布式架构通过灵活、合理的分布式部署策略保证协议/业务处理的高并行度.



正是由于新一代操作系统具备了全业务细粒度分布式架构，因而在构建高可扩展性、高性能、高可靠性的网络方面具有了得天独厚的优势。

2.2 敏捷的实时响应架构

新一代操作系统支持细粒度多进程调度，使得系统不仅能够实时响应网络变化，也能够

实时响应用户需求,为用户带来完美的业务体验。

当前网络承载了语音视频等多种实时业务，这些实时业务对收敛时间有很高的要求。特别是数据中心部署的诸多业务和应用,对收敛时间及时延非常敏感,快速的业务收敛和低时延已经成为数据中心和云计算网络的一大要求. 新一代操作系统针对此需求进行优化设计，配合 BFD 等快速检测技术，使得整个网络硬收敛时间控制在毫秒级，大大降低了网络故障导致业务中断的影响。如果再结合 FRR 技术，用户业务在硬收敛过程中完全不受影响。

2.3 像云般变幻的虚拟化技术

新一代操作系统引入了云计算资源虚拟化的理念,可以根据不同场景将网络资源虚拟化成不同的形态。网络虚拟化在形态上分为“多虚一”和“一虚多”。 其中“多虚一”模式的虚拟化把多个物理网络资源虚拟出一个逻辑资源，比如各种堆叠，集群技术；而“一虚多”模式相反把一个物理网络资源虚拟出多个逻辑资源。

1) 多虚一技术

它可以将 N 台物理设备虚拟为一个逻辑设备，称为多虚一的虚拟化,多虚一技术减少了网络上逻辑设备的数量，简化网络层次，并且提高了设备的扩展能力，更好的保护用户投资,该技术包括华为的 CSS, 思科的 VSS 等;

2) 一虚多技术

一虚多技术是在一个物理网络设施上虚拟化多个相互隔离的网络,从而减少了物理设备数量，提高设备使用率. 以华为新一代操作系统的 VS(Virtual System)特性为例，它提供了网络设备虚拟化的技术架构，实现设备“一虚多”的虚拟化能力，即在物理设备上划分出多个逻辑或虚拟设备系统。每个虚拟系统 VS 就是设备上的“虚拟机”，可以如同单独设备一样独立配置，管理，维护；独立运行，承载网络业务并与其他 VS 相互隔离。数据中心网络通过物理设备上虚拟出来的 VS 承载不同业务或者服务于不同的用户群，达到业务隔离提升网络可靠性和安全性的目的；同时提升设备的利用率，降低用户成本；并可以实现多用户群管理隔离，有效简化运维。

2.4 高可靠性的 NSX 架构

在企业 IT 架构及云网络环境下,突发的软/硬件故障或者重要的软件升级和设备问题修正对于网络的可靠性都是一次不小的考验.一旦在此期间业务中断,将带来不可估量的损失.传统的解决办法是通过增加硬件的冗余来保证设备的可靠性. 而通常容易出现问题的是庞大的软件系统.如何能够提高软件系统的可靠性,软硬双管齐下来保证整个网络的健壮性呢?

新一代操作系统在以下几方面做了细致的考虑和完善的布署:

1) 新一代操作系统在可靠性方面凭借模块化技术可以使软件的各个部分做到故障隔离，保证了一个模块的异常不会影响系统其他部分的运行.
2) 对于突发的软件/硬件故障事件,通过支持NSR技术来自主完成设备主备倒换，同时保证邻居设备感知不到,避免造成路由的间断;
3) 对于设备的软件升级,提供软件不间断业务升级技术(ISSU)来保证升级过程业务不中断;
4) 对于设备问题修正,支持Nonstop patching（NSP）技术来提供设备补丁过程中的业务不中断;
5) 针对设备主备倒换过程中的管理,新一代操作系统支持Nonstop Managing（NSM）技术，实现了主备倒换期间不间断管理能力.使得很多网络问题及时反馈到网管。

华为VRP V8 系统的NSX技术架构，使得设备服务永远在线,为您的网络健壮性提供了强有力保障.

2.5 无法撼动的安全架构

网络设备的安全性无论对于运营商网络还是企业网络都是至关重要的。如果网络设备本

身的安全性无法得到保证，用户数据安全也就无从谈起了。

华为新一代操作系统 V8 的安全架构采用了 High Level Access（HLA）、防沙网和安全日志技术。该架构筑建了层层的防护网，监控网络中的一举一动，能将安全隐患快速识别并隔离,确保网络安全。

1) 高级别接入控制的HLA技术

对于首次上电设备，用户只能通过近端端口登陆设备，并被要求立即更改密码。输入的密码强度需要符合安全规范要求,密码存储在系统中是不可逆的过程，任何人无法通过密码密文反向破解出明文密码.

2) 多层防沙网技术

针对设备攻击中最重要的情形是拒绝服务攻击。该攻击方式通过外部网络发送大量无用报文使得 CPU 繁忙，无法处理正常业务而导致连接中断。另外一种攻击形式是通过端口扫描发现设备的未关闭端口，通过此端口与设备建立大量连接，最终导致系统资源耗尽。

华为新一代操作系统设计了一套独有的多层防沙网技术，来对抗此类攻击。

- 第一层是在转发面直接识别非法攻击流量，并丢弃处理，此类攻击报文根本无法进入CPU层面处理；
- 第二层防沙网是即使正常的上送处理流量，转发平面会进行流量控制。这样当大流量攻击发生时，真正上送到CPU的流量是经过过滤的，不会导致CPU过度繁忙；
- 第三层防沙网是设备内部建立的一个SESSION表，SESSION表内记录了所有由用户配置的和外部连接所需的五元组数据。上送处理会先进入该SESSION表进行判断。如果没有在SESSION表内，则会被丢弃，
- 最后一层防沙网是发生在上层协议开关控制，设备默认的关闭所有端口，这样外部任何非法的连接请求都会被拒之门外。

通过上面的层层筛查，保证了设备的安全性。

3) 让攻击者无所遁形的安全日志SL功能

华为 VRP V8 平台的安全日志包含<黑白名单，登陆记录，系统操作记录>等信息，记录了试图登录系统 IP 地址、试探接入的所有输入和登录进入系统的所有系统操作,用于事后的攻击分析，让攻击者无所遁形,且只有最高管理员才能进行查看和删除.

2.6 简单高效的运维管理

1) 直击问题根源的告警相关性技术

告警是帮助用户及时发现故障解决问题的主动通知机制。但目前一个尴尬的情况是在每天收到的上千条的告警中,有效信息淹没在大量的垃圾告警中,而这消耗了管理员大量的精力与时间.华为 VRP V8 系统的告警相关性方案，彻底解决了你的烦恼。告警相关性是针对告警进行过滤,合并和转换，将多条告警合并成一条具有更多信息量的、确切问题根源的告警,从此烦恼抛掉.

2) 瞬间纠错的配置回退技术

新一代操作系统提供了重大配置调整确认机制——配置回退技术，减少了配置失误所带来的风险，提高系统的安全性与可维护性. 操作人员执行一些重要操作之前可以在不同时间点为系统打上多个标签，每个标签记录了那个时间点的系统状态和系统时间。在遇到配置所引发的故障时,操作人员可以根据当前状态任意选择需要回退的标签点,从此纠正错误就那么简单。

3) 完美仿真的试运行技术

试运行技术是一种减少配置异常风险的技术。对于影响较大或存在风险的配置，用户可以在配置提交时指定这次提交是“试运行”,进入“试运行状态”。用户可以根据系统运行状态来确认配置是否有效、是否对整网业务没有负面影响，然后决定是否取消“试运行”，如果用户执行了确认操作，则试运行提交的配置变为正式配置数据；如果是取消操作，则试运行提交的配置数据将被清除，系统会回退到试运行前的配置。新一代操作系统的试运行技术，能够帮助你实现现网无感知业务验证发放能力，把无法发放可能带来的负面影响降到最低。

3 结束语

通过以上的介绍，我们可以看到新一代操作系统在性能,扩展性,可靠性,虚拟化及维运管理等多纬度展示出来的巨大进步与优势.基于此,使得它在提升网络的性能与容量,提高网络架构的弹性与扩展性,确保网络的稳定运行,简化网络的运营维护等多方面得心应手,非常适应云计算下的业务和应用对网络的要求，符合云计算时代的发展趋势.同时,通过这些革新也降低了用户初期投资与后期维护方面的开支,为用户带来了实实在在的利益与价值.