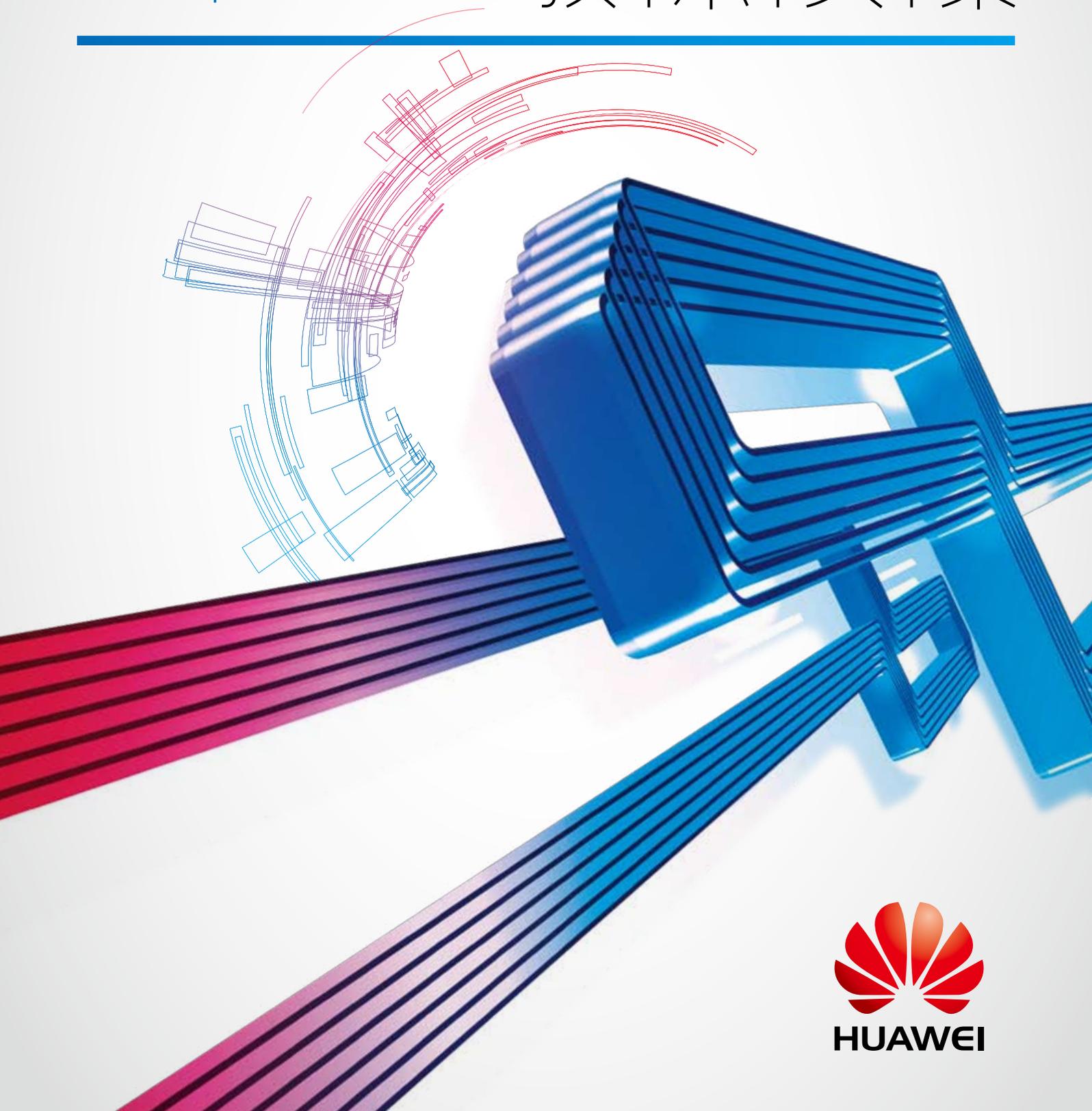


华为

敏捷交换机

技 | 术 | 文 | 集





目录 Contents

01	刊首语 敏捷交换机：从芯开始 改变未来
02	以太网交换机演进史
06	ENP重定义以太转发技术
10	敏捷网络呼唤敏捷交换机
14	复杂留给我 易用带给您 ——快速构建以用户和业务为中心的园区网络
18	华为S12700开启T-bit AC新时代
22	“零接入层配置”让园区网管理更敏捷
24	敏捷的秘密：iPCA网络包守恒算法
28	自在融合，一统有无 ——华为校园网U ² M统一用户管理新方案
34	敏捷交换机开辟未来城域网建设新通路
36	华为视频监控网络护航平安城市
40	华为S12700，高品质VOD网络的巅峰之选
42	如何实现无线园区网络精准规划？
46	基于SDN架构的下一代敏捷园区网

敏捷交换机： 从芯开始 改变未来



作为中国古代“四大发明”之一的活字印刷术对推动整个人类社会的发展与进步起到了重要作用。此前，人们用雕版印刷术来印制和传播信息，该技术存在天生的不足，印一种书就得雕一回版，费时费力，无法迅速大量地印刷书籍。为了克服这些缺陷，北宋人毕昇发明了“活字印刷术”，用胶泥做成四方长柱体，一面刻上单字，烧制成模，排版时将这些字模按照文章的意思排列在一个铁框内，涂墨印刷，印完后再将字模拆出，留待后面反复使用。细细品味，活字印刷术的本质就是打破了雕版印刷术固有的僵化，在印刷技术上引入了敏捷性，字模之间任意编排，造就天下文章。历史具有相似性，技术具有穿越时空的相通性，今天，华为的“毕昇”们，在以太网交换机上也引入了敏捷性，让网络更敏捷地为业务服务。

从芯开始

纵观以太网交换机二十多年的发展历程，每一次变革都根源于业务的变化和技术的发展。

早期企业网络需要传送的是字符、文本，然后逐步有语音、视频，交换机的设计从早期的HUB、二层以太交换机、具备三层功能的交换机到带业务插板的交换机，逐步满足从小的组网、大型组网到承载少量语音和少量视频。对交换机关注更多的是性能，同时要求简单易用，低成本，低功耗。交换机最核心的转发ASIC芯片也是在这样的时代背景下诞生和逐步发展的，在不断追求性能提高的同时，在成本功耗上也占据着明显的优势。

现在企业网络正在发生巨大变化：云计算把应用迁移到云上，网络丢包、时延、抖动严重影响体验；社交媒体和高清视频流量突发、丢包敏感，对网络质量、可靠性、故障定位提出了更高要求；无线接入无处不在，让策略管理和布署变得更加复杂；SDN大行其道，技术不成熟，但它是未来的方向，用户想用新技术却又怕影响业务。新技术层出不穷，企业创新和新业务上线速度加快，新业务从出现到上线缩短到以月为单位；而随着半导体技术的不断进步与成熟，性能早已不再是网络发展的瓶颈。基于ASIC转发的交换机，受制于芯片开发周期，对革命性新业务的支持至少需要24个月，无法适应快速变化。

如何在保证低成本、低功耗的前提下实现业务灵活定制，也就成为业界面临的共同挑战。为了应对这一挑战，华为研发出业界首款专门针对以太网转发的可灵活编程芯片：以太网处理器ENP（Ethernet Network Processor）。ENP

通过内置硬件加速组件、片内集成智能存储和专利高速查找算法，在保留了传统交换机ASIC成本、功耗、性能优势的同时，具备灵活的全可编程能力。

改变未来

华为S12700敏捷交换机，基于ENP芯片，作为敏捷网络的核心部件，与客户一起改变未来：

改变依赖网络迭加来提供新业务的模式，更敏捷地提供业务。S12700融高级路由能力、精细用户管理功能、T-bit AC于一体，改变传统园区网络新业务提供依靠多网迭加的模式来实现，实现有线无线业务的彻底融合，满足802.11ac的带宽要求。传统园区以端口和IP为中心管控各种策略，随着无线化的到来，部署复杂度和周期成倍增加。S12700基于用户为中心进行管控的理念，随板提供了强大的精细用户管理功能，可以方便快捷地部署各种策略。S12700业务能力由ENP编码来实现，既有商用ASIC的性能和功耗优势，更具有无限的灵活性，新业务上线周期仅需6个月。

改变传统网络运维方式，提供精准简化的园区管理方案。基于转发可编程技术的iPCA网络包守恒算法，通过对业务流进行标识、染色和计数，让用户之间的数据流在传送业务的同时，也具备网络质量检测功能。iPCA使无连接的IP网络变得端到端质量自动感知，能够实时故障定位，解决了IP网络故障检测的业界难题。S12700将无线和有线网络虚拟成一张网，甚至可以将整个网络虚拟成一台交换机（WLAN AP虚拟成一个交换机的端口），最大程度地简化了管理、配置。

重新定义SDN交换机内涵，解决SDN技术持续演进难题。S12700可以同时支持传统网络和SDN网络。客户可以将绝大部分业务放在传统网络上，同时虚拟一张SDN网络。当前，在虚拟的SDN网络上，客户可以在无风险的情况下，提前尝试新技术；未来，随着技术的成熟，客户可以通过软件升级平滑支持SDN。当前基于ASIC的SDN交换机，在转发层面上只能支持已知类型报文的转发，而S12700敏捷交换机实现了转发层面的解放，可以任意定义转发模式、转发行为和查找算法，能够响应各种应用诉求，应对现在及未来的挑战。End

文/华为企业网络产品线副总裁 王世宏



以太网交换机演进史

文/徐霆

以太网称霸

作为一种原理简单、便于实现同时又价格低廉的局域网链路层技术，以太网正在成为网络领域的基础和垄断承载技术。40年风雨兼程，以太网逐渐赢得业界普遍认同，成为最有前途的网络技术。这其中，更高性能的快速以太网和千兆以太网的出现，可以说是以太网飞速发展、迅速称霸局域网并将触角渗透到城域网的翅膀。

1973年，施乐帕洛阿尔托研究中心的罗伯特·梅特卡夫(Robert Metcalfe)给他PARC的老板写了一篇有关以太网潜力的备忘录，这被认为是以太网的源起点。1976年，梅特卡夫和他的助手David Boggs发表了一篇名为《以太网：局域网计算机网络的分布式包交换技术》的文章。1977年底，梅特卡夫和他的合作者获得了“具有冲突检测的多点数据通信系统”的专利。多点传输系统被称为CSMA/CD（带冲突检测的载波侦听多路访问），从此标志以太网的诞生。

1979年，梅特卡夫离开施乐成立了3Com公司。3com对迪吉多、英特尔和施乐进行游说，希望与他们一起将以太网标准化、规范化。这个通用的以太网标准于1980年9月30日出台，当时业界有两个流行的非公有网络标准令牌：环网和ARCNET，在以太网大潮的冲击下，它们很快萎缩并被取代。

今天，3Com已经消失，而以太网却呈现出了万夫莫挡的霸气。

四代交换机演进史

从1989年第一台以太网交换机面世至今，经过20多年的快速发展，以太网交换机在转发性能上有了极大提升，端口速率从10M发展到了100G，单台设备的交换容量也由几十Mbps提升到了几十Tbps。凭借着“高性能、低成本”等优势，以太网交换机如今已经成为应用最为广泛的网络设备。

随着以太网的发展，以太网交换机也在持续演进。早期的以太网设备如集线器是物理层设备，不能隔绝冲突扩散，限制了网络性能的提高。交换机（网桥）作为一种能隔绝冲突的二层网络设备，极大地提高了以太网的性能。随着技术的发展，如今的交换机早已突破当年桥接设备的框架，不仅能完成二层转发，也能根据IP地址进行三层硬件转发，甚至还出现了工作在四层及更高层的交换机。

根据交换机工作的协议层次，将交换机划分为：二层交换机、三层交换机和多层多业务交换机，简单回顾一下交换机的发展历程。

交换机前身：集线器

说到交换机，不得不先说一下和交换机外观非常类似的集线器。

集线器（Hub）工作于OSI(开放系统互联参考模型)参考模型第一层，即“物理层”，其主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。



由于集线器收到报文会向所有端口转发，同时只能传输一个数据帧，通过集线器相连的所有主机处于同一个冲突域中，因此，当有多台主机同时发送数据报文时，大量的冲突将导致性能显著下降，这也意味着集线器所有端口都要共享同一带宽，以集线器为核心构建的网络是共享式以太网的典型代表。

严格来说，集线器不属于狭义上的交换机范畴，但由于集线器在网络发展初期具有举足轻重的作用，在很长时间内占据着目前接入交换机的应用位置，因此往往也被看成是（第）一层交换机。

典型产品有：3COM 3C16410集线器、Cisco 1538集线器。

二层交换机

交换机是在多端口网桥的基础上逐步发展起来的，Kalpana公司在1989年发明了第一台以太网交换机，EtherSwitch EPS-700，对外提供7个固定端口。

最初的交换机是完全符合OSI定义的层次模型的，也就是说工作在OSI模型的第二层（数据链路层），因此也被称为二层交换机。二层交换机识别数据帧中的MAC地址信息，主要根据MAC地址选择转发端口，算法相对简单，便于ASIC实现，因此转发性能极高。交换机的出现，解决了集线器的冲突域问题，使得以太网从“共享式”步入了“交换式”时代，大大提高了局域网的性能。

典型产品：Cisco 2960系列交换机、Huawei 5700-LI系列交换机。

三层交换机

在引入VLAN之前，交换机只能隔离冲突域，而不能分割广播域。然而在TCP/IP协议栈进行通信时，广播或组播类型的协议报文会被广泛使用，如ARP/RIP/DHCP等。如果整个网络只有一个广播域，一旦发出广播报文，就会传遍整个网络，这样不仅会影响到网络带宽，而且还会对网络中的主机带来额外的负担。

随着时间的推移，网络由最初的军事、科研用途逐渐融入人们的日常生活，网络用户数急速提升，广播域带来的问题愈发明显。虽然VLAN在交换机上能够实现广播域的隔离，但VLAN之间的转发还是要通过路由器来完成。相对于交换机而言，路由器不仅价格昂贵，而且性能较差，无法满足大量用户对大带宽的需求，人们呼唤能工作在ISO模型第三层的交换机，在满足客户需求的同时继续保持“高性能、低成本”的传统优势。

三层交换机的发展经历了一个小插曲。由于早期的ASIC芯片无法独立完成三层转发的完整功能，2002年左右出现的“三层交换机”采用了广为流传的“一次路由多次交换”技术，逻辑上可以看成在原有二层交换机之上“扣了一个三层的帽子”，因此对外表现为“弱三层、强二层”的特点。但随着芯片技术的发展，很快ASIC就支持了硬件路由查找功能，真正实现了全硬件三层转发的交换机，因此最终“三层交换机”只是昙花一现，很快被全硬件三层转发的交换机所取代。为了避免与前期的“三层交换机”相混淆，支持全硬件三层转发的交换机往往也称为路由交换机。

典型产品：Cisco 3750-X系列交换机、Huawei 5700-EI系列交换机。

多业务交换机

近年来，尤其是万兆以太网出现后，语音、视频、游戏等高带宽业务逐步开始普及，这些业务的开展和部署对网络设备的要求已经不仅仅是完成数据的连通性，还提出了一些新的需求，比如安全性、可靠性、QoS等。同时为了降低组网成本，简化管理维护，网络设备的功能出现了融合的趋势，这就催生了交换机支持多层转发，融合增值业务的能力。

由于ASIC芯片能力的限制，当前的多业务交换机采用了基本二、三层业务“叠加”上层增值业务的混合模型，在组网应用时对外呈现为多台物理设备，本质上是多台设备安装在同一机框内，没有实现真正的融合。因此，这种混合模型的多业务交换机距离客户心目中期望的真正多业务交换机还有一定差距。

典型产品：Cisco 6500系列交换机、Huawei S9700系列交换机。其中Huawei S9700交换机采用全分布式硬件转发架构，单机交换容量最大可达18.56Tbps，最大支持12个业务槽位，支持防火墙/NAT、负载均衡、无线AC、IPSec VPN等多种增值业务能力。

为了便于对比，我们把上面几代产品简单列表如下：

阶段	产品	典型产品	转发硬件	应用场景
第一代	集线器	3Com 3C16410集线器 Cisco 1538集线器	ASIC	共享式局域网
第二代	二层交换机	Cisco 2960系列交换机 Huawei S5700-LI系列交换机	ASIC	小型局域网
第三代	三层交换机	Cisco 3750X系列交换机 Huawei S5700-EI系列交换机	ASIC	中小型局域网
第四代	叠加型多业务交换机	Cisco 6500系列交换机 Huawei 9700系列交换机	ASIC+多核CPU 混合模型	各类园区网 城域网

面向未来网络，第五代交换机呼之欲出

近几年来，云计算、BYOD移动办公、SDN、物联网、视频以及大数据等新概念层出不穷，引发了对高密度、高性能、更灵活、更大规模以太网的需求，由此引发了新一轮以太网交换技术的革命性增长。

总体来说，新业务环境对以太网交换机的期望集中在以下几个方面：

全可编程能力

业务灵活性是当前交换机面临的巨大挑战。为了增加交换机的业务灵活性，厂商往往采用可编程ASIC技术实现多业务能力，但可编程ASIC仅具备部分可编程能力，如自定义报文解析，带来的业务灵活性非常有限，无法完全满足快速多变的业务需求。因此未来的交换机必须具备完全可编程能力才能满足快速变化的业务需求。用户通过升级软件的方式即可支持新业务，而无需更换硬件，保护客户的前期投资。

此外，为了达到简化管理、流量优化、快速部署的目的，SDN也正以不可阻挡之势冲击着现有网络架构，除了当前的Openflow1.3标准，各厂商也都在推出自己的SDN标准。SDN本身也要求下一代交换机必须具备完全可编程能力，确保网络能够平滑向SDN演进。

高度“一体化”

从最早的交换、路由功能融合，到运营商的Triple-Play三网合一（语音、数据、数字电视），再到数据中心的三网合一（计算、存储、通信），网络功能的融合一直是个大趋势，而这背后的推动力都是为了降低组网成本，简化管理维护。

以园区应用为例，WLAN及BYOD的快速发展使得无线用户迅猛增加，而目前无线用户的接入和管理分别是由不同的设备来完成的，这给IT管理和维护人员带来了很大负担，因此迫切要求第五代交换机能够实现无线有线的融合，支持有线用户、无线用户的统一接入和统一策略。另外，随着网络全面步入“以用户为中心”的时代，精细化用户管理也已成为园区网络中不可或缺的一部分。虽然独立BRAS设备在功能上能满足园区需求，但其不菲的价格阻碍了在园区网的应用，因此交换机融合BRAS功能也将是一个趋势。

超大硬件表项资源

到2015年，连接到Internet上的终端将达到33亿，其中70%以上是物联网应用，而随着物联网One M2M标准组织的建立，IPv6应用将进一步在能源、电力、交通等行业扩张。物联网带来了无限连接需求，要求网络设备必须具备更大的表项规格，以适应网络5-10年的扩张能力。

强大的QoS能力

如何保证网络应用端到端的QoS一直是交换机面临的重大挑战。

进入富媒体时代后，网络上承载着大量的实时视频类业务，不仅需要较大的网络带宽，而且对网络的时延和丢包率有着很高的要求。而IP网络的一个重要特点就是流量的不确定性和突发性，为了避免大量丢包引入的时延和额外带宽开销，要求网络设备具备一定的吸纳突发的能力和精细化的队列调度能力。

此外，网络级QoS检测和呈现一直是IP网络的一个难点。在新部署业务时，用户要能够准确判断当前网络是否满足需求；由于网络质量是动态的，在业务运行期间，用户还需要及时感知到网络质量的变化情况，并及时做出响应，如切换到备份链路。

在过去的二十多年中，以ASIC芯片为核心的传统交换机凭借着“高性能、低成本”等优势已成为应用最为广泛的网络设备，然而在面对云计算、BYOD移动办公、SDN、物联网以及大数据带来的变化和和挑战时，ASIC芯片灵活性差的缺点使得传统交换机难当重任，继续在ASIC平台上采用混合模型修修补补也无法延续交换机昔日的辉煌，只有通过变革与创新才能保持交换机的竞争力。要实现交换技术在上述几点的突破，就必须对交换机底层架构进行革命性提升，我们将其定义为**第五代交换机**。End

ENP重定义以太转发技术

文/吕超、彭晓澎

以太转发技术的困境

衡量交换机性能的指标很多，如吞吐量、延时、可管理性、安全性等，而其中最本质的一点，则是交换机的转发技术。

从多年前的十兆到百兆、千兆直至万兆，以太网交换机的转发能力在飞速发展，而ASIC芯片则是为以太交换机的转发能力提供源动力的核心。随着视频、移动、BYOD、云计算、物联网等业务的迅猛发展，以太网本身也在发生巨变。这种变化体现在以太网不仅要具备大规模转发能力，且网络本身要具备弹性、智能控制、管理简易等特性，这就要求以太网交换机的功能要进行灵活、敏捷的扩充。目前，虽然交换机的功能已经由最初的仅二层交换发展到全面支持路由交换，但需求仍然集中在为企业终端提供联通性方面，不能满足云计算下新业务的快速变化，其根本原因就在于ASIC芯片只能识别预先定义的协议类型且转发流程固定。

ASIC的先天缺陷：固定架构无法按需应变

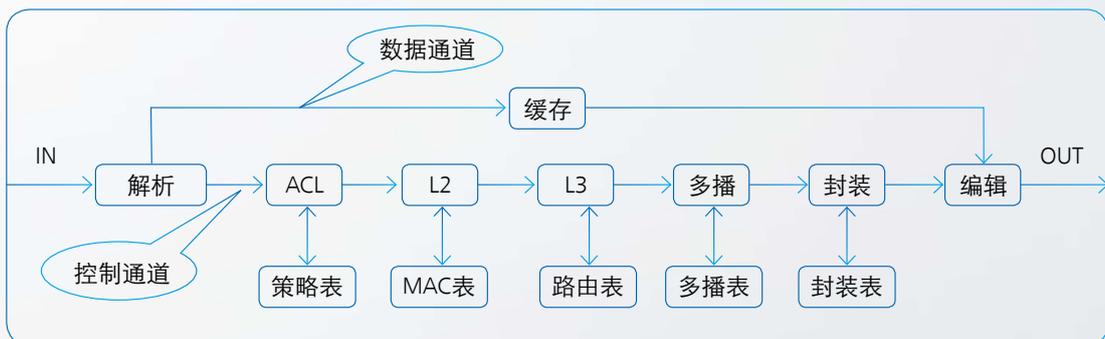


图1: ASIC芯片组成架构

ASIC面临的最大的挑战，就是无法灵活扩展。因为ASIC只能解析预先定义的应用协议，如果要支持新的应用协议，模块内的数字电路必须重新设计，对芯片来说哪怕是增加一个寄存器，整个芯片就需要重新设计。这意味着，每新增一项业务就需要新增一个模块，也就意味着整个芯片需要从头再来。而一个芯片从设计到样片返回，再从样片测试到设备上市一般需要两年以上的时间，这种开发模式阻碍了设备厂商对业务的快速响应。

于是，市场上就应运而生一种ASIC的替代方案——商用NP。那么，商用NP是否能够补上ASIC的短板，成为一种理想的以太网交换机转发核心呢？

商用NP：性能差 功耗大

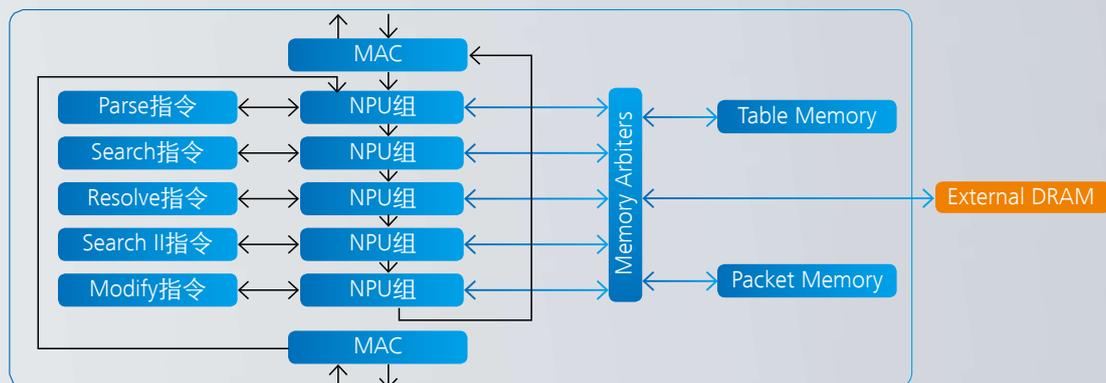


图2: NP芯片组成架构

商用NP一般由五个部分组成：NPU、指令Memory、Table Memory（片内）、Packet Memory（片内）和Table DRAM（片外）。这种设计思路使每个模块的灵活性得到了提高，但是，在实际部署业务时，需要细致地考虑如何进行业务流程切分，而每个NPU组的指令空间都是有限的，如果某个指令空间即将耗尽，则无法支持新的业务。如果业务切分不好，则会导致某些NPU组负载过重，产生业务处理瓶颈，所以实际上NP芯片的总体灵活性并没有比ASIC提高多少，总体性能仍然不能令人满意。

可编程ASIC的诞生，虽然在一定程度上缓解了业务扩展性的迫切需求，但可编程ASIC无法实现完全可编程，只能算是一个过渡方案。到底是继续发展ASIC，还是采取其他的技术？交换机转发芯片的前进之路究竟在何方？



ENP：性能和灵活性的完美结合

ASIC性能高、功耗小，但架构固化不灵活，无法适应企业IT应用的快速发展；商用NP虽然灵活，但性能和功耗却成为瓶颈。针对这种现状，华为公司立足于二十多年芯片研发积累，开创性地推出了以太网网络处理器ENP，其性能和功耗比ASIC，同时具有商用NP的灵活性，是性能和灵活性的完美结合。该芯片具有以下一些卓尔不群的特点：

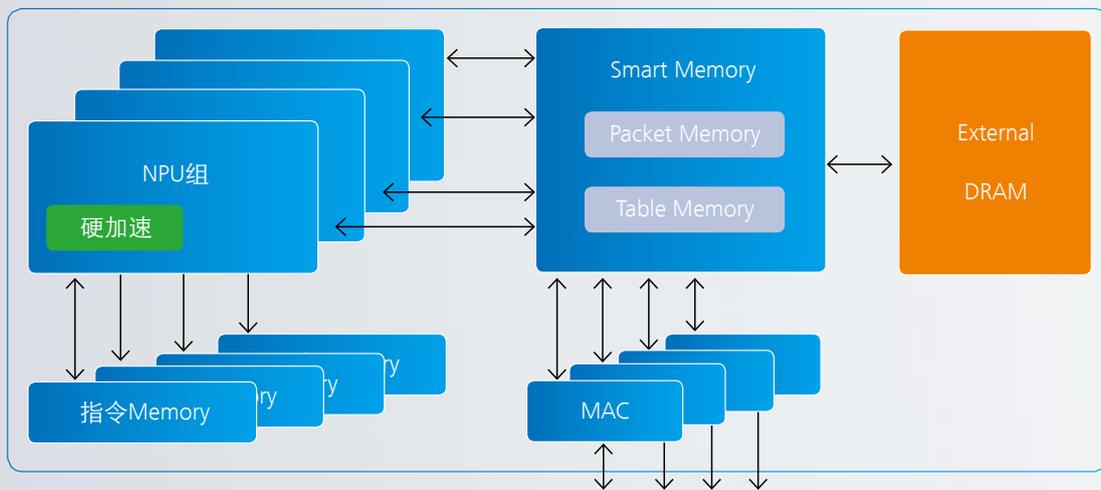


图3: ENP芯片组成架构

1、完整的指令空间与硬加速，克服了商用NP的性能短板

ENP中的NPU与商用NP中的NPU有所不同，可访问完整的指令空间，因此每个NPU组都能执行从Parse到Modify的任何指令。这样就不需要像商用NP那样，将业务处理切分到不同的NPU组上，节省了开发过程，可以快速开发出新业务。另外，ENP采用了多线程技术，有效降低了IO访问延时对NPU性能的影响。

2、华为SmartMemory，解决了内存访问的性能瓶颈

商用NP或商用ASIC在架构上将计算与存储严格分离开来，导致计算逻辑单元与存储单元物理距离增大，计算单元和存储单元交互增多，进而导致访问延时大，功耗高。如果多个源对同一地址进行读写操作，为保证数据的一致性，必须锁存地址，这样很容易形成访问瓶颈。针对这种情

况，华为ENP集成了SmartMemory，让存储单元集成了一些计算和判断处理的能力，用以减少主计算单元与SmartMemory之间的操作交互，大大提高了计算单元与存储单元之间的访问效率。

另外，SmartMemory还集成了华为自研的查找算法引擎（Search Engine）、协处理器（Co-Processor）和流量管理器（Traffic Management），囊括了商用NP或ASIC对内存操作的所有算法，如查找、运算、读写等等，可以被ENP任何功能单元(如流量限速、统计)所调用。

3、百万级别流表，全面支持Hybrid Openflow

基于Hybrid Openflow的SDN网络方案，采用Openflow和传统路由双平面来进行不同的转发控制，用于传统网络向SDN进行过渡。通过可编程的方式和高达16M的流表资源，基于ENP的交换机可同时支持Openflow和传统以太网数据包转发，帮助用户实现从传统网络向SDN的迁移。



4、先进的降功耗措施使得ENP具有和ASIC比平的能耗表现

ENP可以从三个方面降低设备功耗。

首先，ENP集成度高，一个ENP可完成多个芯片的功能。交换机的功耗主要来源于设备内的芯片，芯片数量越多整机的功耗就越高。一般来说，完成大表项和大缓存功能需要用分离的两个芯片来完成，一个完成转发，另一个用于报文缓存。而华为ENP将两颗芯片集成为一颗芯片，有效地降低了功耗。

其次，通过业界先进的电压控制器来减少静态功耗。芯片的功耗由两部分组成，一部分是静态功耗，另一部分是动态功耗，前者占总体功耗的40%，后者占60%。静态功耗与晶体管工作电压成正比，晶体管工作电压可根据各芯片在加工过程中形成独特的电气属性来调整。

最后，可通过改变晶体管工作电压和时钟频率来降低动态功耗。ENP集成华为独创的测速器，可以检测芯片内部流量，自动调整工作时钟频率。例如原有的时钟频率是400MHz，若降低到300MHz，则动态功耗会降低到原有的75%。另外，当流量减少时，还可以关闭空闲的NPU组来减少功耗。

选择ENP 选择未来

以太网在向更敏捷、更智能、更安全、更高速、更高服务品质的方向持续演进，新一代以太网产品和技术山雨欲来，灵活敏捷、智能应对业务需求是新一代以太网络的核心竞争力。而以太网交换机对于数据、语音、通信、视频、移动等综合的敏捷支持迫在眉睫，华为站在市场前沿，以前瞻性创新为起点所带来的ENP芯片，既能像商用ASIC那样提供线速的转发能力并保持低功耗，同时又比商用NP更灵活，必将重新定义以太网转发技术，成为新一代以太网交换机的核心转发技术标准。 **End**

敏捷网络呼唤 敏捷交换机

文/杜平周

你好，敏捷网络

沉寂多年以后，以太网进入了新一轮令人激动的技术创新演进期。云计算、移动互联网、视频、社交网络、物联网等新型应用呈井喷式发展，引发了新一轮交换技术从性能、架构、服务质量、智能管理乃至绿色节能等各个领域的创新潮。

创新应用催生敏捷网络，需要更快速度、更平坦架构、更智能能力，这是业界共识。例如，云计算要求网络要具备可控制的虚拟资源可伸缩性，而这一点，是传统ASIC芯片所不能支撑的，需要具有思考能力的智能芯片提供“芯”能力才能实现。再比如，传统以太网交换机不具备内置的故障定位和性能监视能力，发生故障时难以精确定位，而网络应该能自动发现网络故障并精确定位，还应该能测量端到端性能，实时掌控全网运维状况。网络还可以把一个IP网络虚拟为一台交换机，实时掌控、自动发现新加入的业务节点并自动配置等等。

总的来说，敏捷网络应该具备以下几个特征：

- 颠覆业务发展模式：资源可控性伸缩，即全网资源虚拟化，而不是设备虚拟化；SDN ready；
- 策略随行：整体IP网络资源可管理、可移动，即资源全网策略随行；
- 运维创新：网络可感知，具备全局安全协防能力。

敏捷网络技术层面基本诉求

首先，更高可靠性。随着BYOD、桌面云、SDN等企业业务的发展，企业网络不仅包含接入固定用户、无线用户，还包含接入远程的VPN用户，接入用户数量日益增大，对企业承载网络的可靠性要求也日益提高。尤其是企业网络的核心交换机，一旦出现故障将大范围影响企业业务，因此，“高可靠性”成为企业核心交换机的首要需求。

其次，敏捷可编程性。企业业务的变化速度远超过去，快速的业务发展和较长的网络部署周期之间的矛盾日益显现。企业的业务2-3年就会发生一轮变革，而网络设备一般需要5年以上的时间才会更换。通过可编程满足新业务的发展，从而规避频繁的网络设备更替。

第三，更强表项能力。目前，IPv4地址基本耗尽，IPv6地址逐渐增多，网络设备的IPv4/IPv6地址共存。由于IPv6地址占用的表项资源是IPv4地址的两倍甚至更多，要求交换机在同样地址数量的情况下具备更强的表项能力。其实就是要求核心交换机具备高可扩展性，通过扩展满足未来业务的表项资源要求。

华为S12700敏捷交换机三大优势

企业核心交换机如何满足高可靠性、高扩展性以及可编程能力等这些新诉求？这是摆在所有网络交换机厂家面前重要的课题。华为公司针对这些新诉求，推出新一代基于核心路由器平台技术的S12700敏捷交换机，满足未来网络基本诉求。

首先，S12700 CSS2借鉴核心路由器的硬件交换网集群技术实现了网络级的高可靠性。网络设备的高可靠性具体表现在主控的可靠性、单板的可靠性、电源的可靠性、风扇的可靠性等，这些都是单个设备的可靠性，基本上现在的高端交换机都具备了这些能力。而更重要的是整网的可靠性，即如何通过网络架构保证整个网络的可靠性。华为在S9700/S7700系列交换机中独创了CSS技术，通过主控的交换网直接出集群口，很好地保证了网络的可靠性。S12700在CSS基础上参考核心路由器的交换网集群进行了改进，推出新一代集群技术CSS2（Cluster Switch System Generation2）（如图1所示），通过交换网板直接出集群接口进行互联。每个交换网可以支持8×10GE集群子卡，集群带宽640G，未来可升级到

6×40G集群卡，堆叠带宽可以达到1.92T，远超业务口集群的堆叠带宽。相比业界集群的两次交换，CSS2技术仅需数据跨框一次交换，时延仅为21us，是业界最低跨框时延，仅为业界平均时延的60%。另外，在堆叠的情况下，使用业务口集群的传统网络厂家都要求每个交换机至少要有—个主控，而CSS2独创了单主控管理整个集群系统的技术，可做到整个集群只要有一个主控，系统即可正常工作，实现主控的“1+N”备份。上述两项技术目前业界主流厂家都无法做到。总之，华为S12700的CSS2硬件集群方式从集群本身、主控“1+N”备份等多个方面最大可能地保证了网络的可靠性。

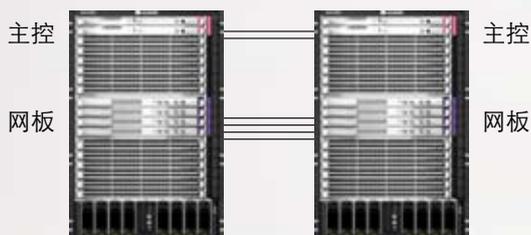


图1: S12700 CSS2架构连接示意图

其次，S12700采用了华为自研的ENP (Ethernet Network Processor)芯片，具备全可编程能力。ENP芯片是华为公司针对以太网定制的新处理器架构，既继承了传统NP的灵活性和表项缓存，又在功耗、性能等多个方面取得了突破，达到了可以和ASIC芯片相匹敌的能力（如表1）。

芯片	性能	灵活性	集成度	功耗	表项
ASIC	高	低	中	低	低
商用NP	中	高	中	高	高
ENP	高	高	高	低	中

表1: ENP/NP/ASIC优势对比

S12700敏捷交换机的核心优势在于ENP芯片的全可编程能力，可以通过微码的持续升级改变转发架构和流程，一次投资，满足10年的业务诉求。在可编程业务的支持上，S12700在交换单板内置了AC和BRAS业务能力，在实现有线无线融合的同时，增强了用户管理能力。另外，S12700不仅能在控制面提供对外接口，更重要的是能提供灵活的转发面可编程，各种转发资源、转发流程、报文封装等都可进行编程，相对于传统ASIC固化的流程，S12700将更好地支持未来SDN的发展。

第三，S12700借鉴高端路由器的业务能力，实现了高可扩展性。S12700推出四块主流板卡（48口GE光、48口GE电、4口万兆口+24GE光+8Combo、8口万兆卡+8Combo）。主要表项能力如图2所示，达到普通商用ASIC板卡的数倍。其中，大的路由表和MAC表可以很好地满足IPv4/IPv6混合组网以及未来物联网对于表项的需求。大Buffer能力能够很好地解决高速业务的突发和拥塞，比如高清视频的传输，数据中心环境下的大数据搜索，批量图片拷贝等。



分类	MAC	ARP	FIB	Netstream	Buffer
华为X1E板卡	1M	256K	3M	1M	1.5G
商用ASIC板卡	512K	64K	512K	8K	8M
倍数	2倍	4倍	6倍	128倍	192倍

表2: S12700 X1E系列板卡规格对比

另外，随着以太网语音、数据、视频等有线和无线流量的快速发展，网络中同时传输着不同用户的多种业务组合，不仅不同业务对于网络的保障要求是不同的，而且不同用户之间的同一业务优先级也是不同的。比如从业务上来看，语

音对于网络的要求肯定要比普通数据高，而智真系统对于网络时延等的要求又要比语音高；而从用户来看，VIP客户的优先级要比普通客户高。S12700支持五级的HQoS，不仅可以基于业务调度，还可以分层次来进行不同用户、不同业务的QoS部署。大容量的Netstream流表可以很好地分析企业网的流量，提供可视化应用。S12700的板卡具备的这些高可扩展性为企业业务的发展提前做好能力和资源上的准备。End



复杂留给我 易用带给您

——快速构建以用户和业务为中心的敏捷网络

文/沈宁国

BYOD兴起，企业根本难以阻止这个趋势。有统计数字表明，自带设备办公已经在商界取得重大进展，有60%的员工已经在工作中使用自己的技术设备。类似的新应用层出不穷，对企业的网络提出了全新挑战：社交化、无线化、广域化和开放化。

这种背景下，快速构建以用户和业务为中心的敏捷网络成为许多企业的难题。网络的要求千变万化，但其核心是要求网络的运维方式从原来“以设备管理为中心”转变到现在“以用户管理为中心”。做出改变并不容易，因为基于用户的管理将网络管理从一个相对静态的结构转变成相对动态的结构，极大地增加了网络的不确定性，也会同步提升网络管理的复杂性，对于企业用户来说，这可能是致命的。如何实现像Apple的iPad一样，“将复杂留给厂商，将易用带给用户”，这对网络厂商提出了更高的要求。



汹涌而至的新“四化”

毫无疑问，每一个企业都在面临巨大的变革浪潮，而其中四个不可忽视的关键词就是社交化、无线化、广域化和开放化。

- **企业应用社交化：**企业可以构建自己的社交网络，通过社交网络提高分享、沟通、合作的能力，允许员工在任何时刻访问内部社交平台，发布个人问题，寻求解决方案，或者帮助他人解决问题，可有效提高内部沟通和解决问题的效率。
- **企业网络无线化：**用户使用的网络终端不再局限于台式PC或者笔记本电脑，各种智能终端都能成为办公应用的主要载体。这些终端接入无线网络最可行的方式莫过于WIFI，企业需要在内部通过WIFI构建自己的无线网络。
- **企业应用广域化：**随着企业经营的国际化、分工的精细化和管理的IT化，企业的IT系统不仅需要覆盖全球的分支机构，覆盖上下游的客户/供应商，还需要支持员工任意位置的接入要求。这些广域连接构成企业网络的一部分，使得企业网络不断地向外延伸。
- **网络开放化：**无线化和广域化都迫使网络更加开放，而开放化的网络直接挑战着企业网络的安全基础和安全模型：向用户提供接入开放网络的手段，同时根据接入用户、终端、软件环境赋予恰当的权限，进行严格控制。

新一代企业网演进图

传统的企业网络架构在面临挑战，处在社交化、移动化、开放化、广域化等新业务需求交织环境中的企业网络该往哪个方向演进？

融合无线有线网络的统一策略，更友好的视频体验，灵活、可扩展、支持更多设备无障碍接入的无线网络，支持更高容量的同时降低运营成本，丰富的IPv6支持功能，简化的运营和网络管理，网络资源可精确感知性等，都是企业对未来

网络建设的要求，而目前多数企业的需求集中在以下几点：

1) **网络无缝覆盖：**传统网络仅在办公区域通过有线接入进行全面覆盖，无线仅覆盖内部的少量区域，例如会议室。这种覆盖方式不支持员工的BYOD，也不利于社交网络永久在线。下一代的网络需要在办公场所同时提供有线接入（Ethernet）和无线接入；需要支持远程接入，允许用户从外部接入网络。网络无缝覆盖允许员工和合作方员工在任意时间、任意地点连接到网络。

2) **用户身份和使用终端的精确识别：**传统网络中，实施的是基于有线交换机端口的认证。BYOD引入后，网络无缝覆盖，需要网络设备能够精确识别用户身份、终端类型和使用环境，有针对性地对用户实施安全策略和业务保障策略。

3) **支持富媒体：**未来企业网络不仅要支持传统的数据和语音业务，还需支持富媒体业务，特别是实时视频类业务，以有效提升沟通效率，降低沟通成本。和语音不同，实时视频业务对时延、带宽和丢包率（视频质量）同时存在较高的要求。传统视频业务必须通过构建专网才能提供，而在新一代的企业网络中，用户需要在任意终端上获得实时视频服务，专网的方案并不可行，因此，实时视频业务的识别和保障就成为网络的必然要求。

4) **灵活权限控制和访问记录：**传统网络受限于廉价接入交换机有限的权限控制功能，只能通过VLAN实施粗略的访问控制。而敏捷网络需要针对不同的用户、不同的终端实施不同的权限控制，要求网络设备具备超强的用户权限控制功能；另外，在开放的网络中，需要对用户行为进行详细的记录，以备事后审计使用，这要求网络设备具备强大的流分析和记录的能力。

5) **受限的投资，简化的管理：**虽然网络的功能需要不断强化，但网络在企业内部始终是一个边缘的基础设施，不仅投资受控，网络管理人力

也有限。这决定了企业不可能接受一个全新的、较高成本的网络架构，也不能接受一个对管理工作提出全新要求的解决方案。因此，保持原有解决方案最大程度地兼容现有网络，并能够简化网络管理成为敏捷网络成功的关键。

以用户体验为核心，华为S12700的BRAS秘籍

华为在最新推出的S12700系列敏捷交换机中引入了全球领先的BRAS用户控制、业务提供和管理简化组件，面向企业网，开发出专门针对BYOD的全新业务处理单元，能够帮助用户快速完成网络升级。

以ME60为代表的华为BRAS为中国电信数以亿计的用户提供了精细、简洁、高质量的宽带远程接入服务，这些成功的经验和深厚的技术积累，

指引着华为在企业网络市场上进行另外一番创造：华为公司最新推出的S12700系列敏捷交换机引入了全球领先的BRAS(ME60)的用户和业务管理组件。

S12700的部署完全兼容企业现有的网络，广泛部署的接入汇聚设备无需进行升级或者改造，仅需升级核心汇聚设备，即可引入强大的用户管理功能，提供全新的业务。而集中化的用户管理机制，又可以大大降低用户和业务管理的工作量。总的看来，S12700包括以下一些创新的特性：

1) 有线无线用户统一接入，本地远程用户统一认证。S12700同时支持有线用户接入、无线用户接入和远程用户接入；支持全面的认证技术，允许用户通过各种认证方式接入；S12700能够精确地识别用户，并对用户进行全方位的安全保护。

2) **用户上下文识别机制**：S12700内置精确的终端识别机制，配合外部的服务器，能精确地对用户的终端类型、软件版本、软件环境（恶意病毒软件）等进行检查。

3) **用户策略集中控制机制和策略下发机制**：S12700能接受统一的授权服务器的管理，对用户实施完整的权限控制和服务质量保证机制。

4) **业务保障**：S12700引入ME60针对用户/业务粒度的五级层次化调度机制，能够精确识别业务，并对用户业务实施细颗粒的保障，有效保证实时视频业务的质量。

5) **审计检查**：S12700支持大容量的NetStream，能够对用户的网络访问行为进行全面记录，用于事后检查和审计。

6) **业务定制**：基于华为公司首创的ENP以太网处理器，S12700可以简单地通过升级软件来定制出不同的业务处理逻辑，满足不同业务诉求。

未来无限，S12700开启敏捷网络之旅。 



华为S12700开启 T-bit AC新时代

文/张君光



2013年2月，Dell'Oro集团发布一份市场报告，预测到2017年WLAN市场营收将超过110亿美元，比2012年增长将近50%。

无线网络，前途无限。

推动无线网络指数级增长的原因，包括服务提供商部署WLAN、企业移动应用激增、基于无线的视频业务突飞猛进、BYOD以及802.11ac的更新换代周期等。而新应用对现有网络架构也提出了许多挑战，诸如有线和无线融合管理的统一策略就是一大挑战。另外，越来越多的功能捆绑到AP或AC中，导致用户的成本不断增加。

与以前相比，无线网络还出现了一种趋势，那就是越来越多的大企业开始把WLAN视作可运行关键业务的生产型网络。目前业界部署的无线网络多为瘦AP架构，需要AC来做数据集中转发，因此AC的转发性能至关重要。随着BYOD的兴起，无线办公成为趋势，企业的无线网络规模日益增大，与此同时，IEEE802.11ac千兆无线网开始逐渐普及，AC的性能越来越成为网络瓶颈。如何应对，是摆在整个业界面前的一个问题。

AC性能：客户最头疼的问题

无线网络规模膨胀，AC容量免为其难。随着无线办公的普及、BYOD的兴起，企业的无线网络在急剧增大。按照覆盖范围来讲，从最开始的点状补充(如独立的办公室、会议室等)，无线网络只作为有线网络的延伸，到面状全覆盖，企业内部到处覆盖无线信号，无线网络成为办公主体。从最开始一个企业部署几个、几十个AP，到目前的几百、几千个AP。以一个2万员工的大型企业为例，每位员工除了公司配备的笔记本外，还会有个人的PAD、手机智能终端等，因此，1个员工平均持有2~3个终端。2万人的企业则有4万个以上的终端，按照平均每个AP覆盖20个终端，则需要部署2000个以上AP。业界目前单台AC的管理容量一般在1000个AP左右，多为256~512个AP，要管理2000个AP，则至少需要2~3台独立AC，如果再考虑AC备份，起码需要4~6台AC，这么多AC的部署和管理给企业带来了很大的建设运维成本。

802.11ac大带宽，AC性能捉襟见肘。802.11n的3*3MIMO带宽仅为450Mbps，而802.11ac 3*3 MIMO时空口带宽则达到1.3Gbps，提升了3倍；另外，11ac的编码效率更高，除去空口开销，实际可用带宽达到1Gbps，跨越了有线无线之间的带宽鸿沟，给企业无线应用带来了广阔的前景，然而，这也给负责集中转发的AC造成了很大的性能压力。以2000个AP来计算，按照3:1收敛，AC的转发性能就需要： $2000AP \times 1Gbps/3 = 660Gbps$ ，而目前业界AC的集中转发性能约为10Gbps，远远无法满足11ac时代的业务要求。

业界解决方案的三大缺憾

当单台AC转发性能成为瓶颈时，一个自然而然的做法就是增加AC节点，如增加独立盒式AC或框式AC插板，但这种做法总是有这样和那样的缺憾：

缺憾一：网络预留资源不足

在业界主流部署方式中，AC是旁挂在汇聚交换机旁，因此在增加AC节点时，需要汇聚交换机提供更多的端口，而在企业原先的网络规划中，汇聚交换机往往没有为AC预留额外的设备空间和端口，这导致增加AC节点非常困难。

缺憾二：AC节点增多，难于管理

增加AC节点的同时会给管理带来很大的不便，本来数据集中在一台AC，只需要配置一份，而新增多个节点后，则需要配置多份数据，还要保证相互之间的一致性。当需要调整配置时，多个节点要同步进行，容易出现差错。而且，AC节点增多，相互间的故障保护难以有效实施，可靠性不能保证，更重要的问题在于AC是无线网络的核心，一旦故障，则会造成整个无线网络的瘫痪。

缺憾三：有线无线叠加网络，运维成本高

现有的网络部署中，WLAN无线网络是叠加在有线网络之上，这两个网络需要分别进行数据配置、策略控制、网络管理等等，运维成本高。另外，虽然业界有框式AC，但是每块板卡相当于一个独立的AC节点，只是借用了交换机的插槽和电源，没有真正地实现统一管理。

华为S12700随板AC的三大优势

华为S12700敏捷交换机，采用高性能的ENP以太网处理器，有效解决了AC性能瓶颈，开启了T-bit AC时代。

业界首款T-bit AC

传统的AC功能要么由独立的物理设备来实现，要么就由框式交换机的独立物理板卡来完成，而S12700随板T-bit AC是基于ENP技术，融合AC处理和以太交换为一体，每块板卡支持80G线速转发，是业界独立AC性能的2倍以上，整机更高



达960Gbps线速转发，整机可以提供高达T bit/s的CAPWAP隧道封装/解封及二层/三层数据转发能力，相比于传统独立的AC，无论是管理AP数还是用户数，都有数倍的提升。

随板AC，节约用户投资

用户无需购买AC设备或AC板卡，只要利用S12700随板AC和随板BRAS的功能联动，就可实现有线无线用户的统一管理，既简化了网络部署，又节约了投资。另外，内置的随板AC不需占用额外机柜空间和端口资源，节省用户对机房建设的投资。最后，华为S12700随板AC可扩展性好，随着企业无线网络规模的增大，只要通过增加板卡即可实现平滑升级。

有线和无线的真正融合

华为S12700随板AC，创造性地将“AC管理AP”的优秀实践应用到“核心交换机管理接入交

换机”上，具有随板AC功能的以太网业务接口板，不仅负责有线无线业务的统一转发，还对AP和有线接入交换机进行统一设备管理，集中配置下发，在业界第一次实现了有线和无线网络的统一管理、统一策略和统一转发，做到了有线和无线网络的真正融合，大大降低了企业的运维成本，促进了企业的IT业务创新。

未来即将到来

随着WLAN技术的发展，当11ac采用4*4 MIMO 160Mhz频宽时，带宽可达到3.5G，集中式的AC将难以满足带宽需求。华为即将推出层次化AC解决方案，上层通过云AC实现整网AP和业务的统一管理，下层通过汇聚交换机实现就近转发无线流量，降低对集中式转发的AC性能要求。 **End**

“零接入层配置” 让园区网管理更敏捷

文/张俊

数据中心网络炙手可热、创新不断，相比之下，园区网似乎是被遗忘的角落。云计算、SDN、扁平网络架构、虚拟化、新型运维管理策略等热点驱动着数据中心网络架构变革，园区网作为企业网络的传统核心领地难道真的无动于衷吗？

“园区网市场表面上看似平静，其实并不平静，它正在经历一个质变的过程。园区网建设是业务驱动的，现在新业务层出不穷，这些新业务都要求园区网在带宽、可扩展性、可靠性、移动性、安全性、网络管理等领域进行相应的技术创新。而华为认为，无论技术如何发展，核心都是要使业务与网络能深度协同，例如云计算与园区网弹性化的协同、多媒体业务与网络可靠及可视的协同、BYOD与无线和安全的协同等，通过这些深度的协同最终帮助企业提升效率和收益、降低TCO。”

华为企业网络产品线副总裁李向军说。

ZK Research的首席分析师Zeus Kerravala说：“云计算将改变园区网，因为云计算带来了新的网络流量。传统上，园区网只是进出本地数据中心而已，而云计算意味着网络流量将从分支机构或园区直接通向云。这将对园区网核心和骨干网络提出更高要求。”

这其中，园区网的运维管理更加需要新思维。



园区网的“补丁危机”

典型的园区网由核心交换机、汇聚交换机和接入交换机组成，一个园区网少则需要数十、数百台接入交换机，多则上千台。每台接入交换机需要配置端口VLAN、网管IP地址、ACL和QOS等参数，当软件升级或打补丁时，需要逐个操作，工作量大，容易出错。

园区网的重要挑战来自无线消费设备数量的不断增长，如iPad和Android手机。园区网需要更加强壮的WiFi来处理更多的流量。随之而来的就是WLAN在园区网中日益广泛的部署，AC+瘦AP组成的WLAN网络架构日渐成熟。一方面，AC是WLAN系统的设备管理控制器，对AP进行配置管理，而AP为用户提供无线WLAN接入服务。AP功能精简，即插即用，实现零配置，其所有的配置和管理全部集中在AC上，AP也不再作为独立的网元。另一方面，AC是WLAN网络的策略控制器，AC从策略服务器上获取相应的策略后，通过CAPWAP隧道把策略下发给AP，由AP来执行无线用户的管控策略。WLAN网络的这种主从模式，大大减少了AP配置工作量，便于AP软件升级，可更有效地执行策略控制。

有线无线网络融合的过程中，华为成功地将“AC管理AP”的优秀实践应用到“核心交换机管理接入交换机”上，使整合后的园区网络更加有效、简洁，让客户轻松应对网络管理，尽享网络之乐。

首创“零接入层配置”

在这个数据为王的时代里，当大量的生产和经营数据集中在有线无线融合的网络上，网络的运维管理就需要针对园区网基础架构的变化做出改变，做到与网络架构齐头并进。例如有线无线网络统一管理、统一配置等一致性策略，就显得格外重要。

以S12700敏捷交换机为核心，华为推出了业界首个“零接入层配置”方案，把无线（AC+瘦AP）的简化管理模式应用到有线网络，解决了大量接入交换机的重复配置问题。通过提取出有线和无线的相同属性，制作统一的用户或网络模板，实现有

线无线管理模型统一，使维护人员不必再熟悉有线和无线两套配置命令，节省运维成本。



开局零配置

如上图所示，接入交换机和AP一样，通过CAPWAP隧道从S12700内置的有线无线统一控制器中下载配置，S12700统一管理AP或接入交换机等接入设备，实现开局零配置。

自动升级

S12700敏捷交换机保存了接入交换机和AP的版本文件，可根据设备的MAC、IP地址、用户数量、接入端口UP数等，按照业务需要自动升级，避免了批量升级时由于调度无序带来的网络拥塞问题。

即插即用

接入交换机或者AP故障后，可根据网络拓扑结构，使新接入的交换机或AP从S12700上自动同步版本和配置，不必再做任何操作，实现故障更换后即插即用。

一体化模板

统一有线用户和无线用户的认证方式，统一用户认证前、认证后的策略配置模板，通过S12700下发给接入交换机和AP，解决有线无线两个配置模板所带来的运维繁琐问题，保证有线无线用户的一致体验。End

敏捷的秘密： iPCA网络包守恒算法

文/刘碧

敏捷网络的“可视化”渴望

随着网络越来越复杂，对于网络管理的需求也在发生变化。我们看到，网络管理在朝着几个方向发展，如可视化、自动化、智能化等。尤其可视化对于端到端的流量透视以及全网的安全策略管理等网络整体性能管理和运维至关重要，成为网络厂商的新发力点。

Gartner的调查结果表明，“主动预防网络性能问题”是当前企业客户首要的运维投资驱动力，占整个投资的27%，而“快速网络故障诊断”、“业务质量保障SLA”分别排在第二、第三位，其投资驱动力分别为15%、12%。

传统上，IP网络运维存在多点“不可视”。例如，业务性能不可视，也就是说传统网络管理只提供网络的性能，看不到网络上的承载内容，导致故障认知盲点多，故障定位效率低。再如，传统网管路由不可视，看不到业务路径，导致运维人员无法预防路由振荡引起的全网故障。

是否有方法彻底解决网络运维中的上述“盲点”？

在华为看来，首先要转变思维，将传统的被动网络运维转变为主动网络运维，实现对终端用户的业务体验监控，对潜在的故障点和薄弱环节进行精确判断，才能做到科学、高效的“水来土掩、兵来将挡”。



传统故障检测的“罩门”

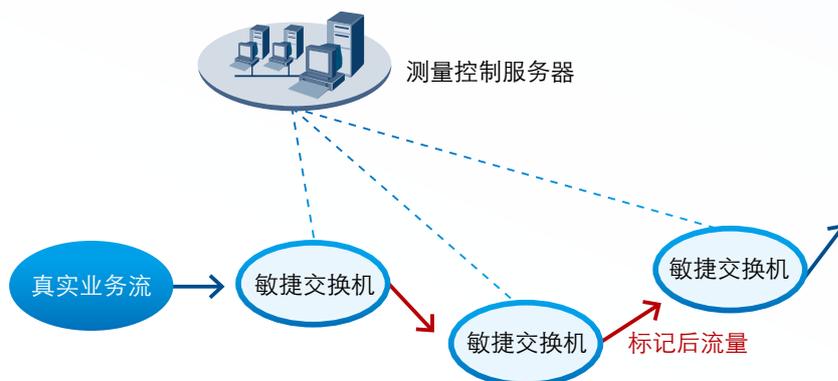
网络故障诊断和质量评价等问题是网络维护的核心问题之一。通常情况下，IT管理员不能确定网络是否有故障隐患，也不会知道在哪里发生了故障，因此对视频、语音和上网等业务性能质量无法客观评价。传统园区网业务的性能故障诊断缺乏有效的E2E定位手段，导致故障诊断时间长、难度大，难以满足用户要求。

网络性能故障诊断和质量评价十分重要，目前有多家研究团体和标准组织从事技术研究和标准制定。IETF制定了RFC5357（A Two-Way Active Measurement Protocol）和RFC4656（A One-way Active Measurement Protocol（OWAMP）用于IP网络的性能统计和故障检测。与此同时，Cisco推出了私有的SAA（服务保障代理）方案，华为公司则采用NQA（网络质量分析）机制，以响应IP网络可维护、可运营的诉求。所有这些用于IP的故障检测机制有一个共同特点：它们都是一种间接测量方法，需要通过插入专用的检测报文，计算检测报文丢包率来间接推导出业务丢包率。而IP通信是无连接的，检测报文经过的路径并不一定就是业务报文经过的路径，这导致检测出的路径质量不能真实反映业务报文的传输状况。

网络包守恒算法iPCA

企业园区网络的运营维护不仅仅要关注网络功能和性能，更要从用户与业务对网络的要求出发，关注用户体验和网络质量。华为S12700敏捷交换机的iPCA提供的网络包守恒算法，能够快速检测任意用户的视频、语音等业务质量，即刻定位故障发生在链路、板卡甚至芯片的位置，大大提升了运维效率。网络能用与好用是完全不同的两个境界，iPCA无疑实现了从“能用”到“好用”的飞跃。

iPCA（Packet Conservation Algorithm for Internet，网络包守恒算法）是一种基于直接测量方式检测网络质量状况的管道监控类技术，它可以测量网络的丢包、时延、时延抖动和流量，并通过逐跳检测，完成故障精确定位。针对现有的检测手段存在故障定位时间长、故障定界模糊和评估精度差等问题，华为新推出S12700敏捷交换机，利用其灵活可编程的特点，开创性地实现了iPCA功能，全面提升网络质量检测 and 故障精确定位能力，降低网络运维成本。



iPCA原理示意图

如上图所示，iPCA方案包括两部分：测量控制服务器和敏捷交换机。测量控制服务器接收用户对目标业务流进行质量检测的请求，通知敏捷交换机进行检测，收集各个敏捷交换机的统计信息，计算并形成报告。

总体说来，iPCA具有以下特点：

华为专利技术，解决IP运维业界难题

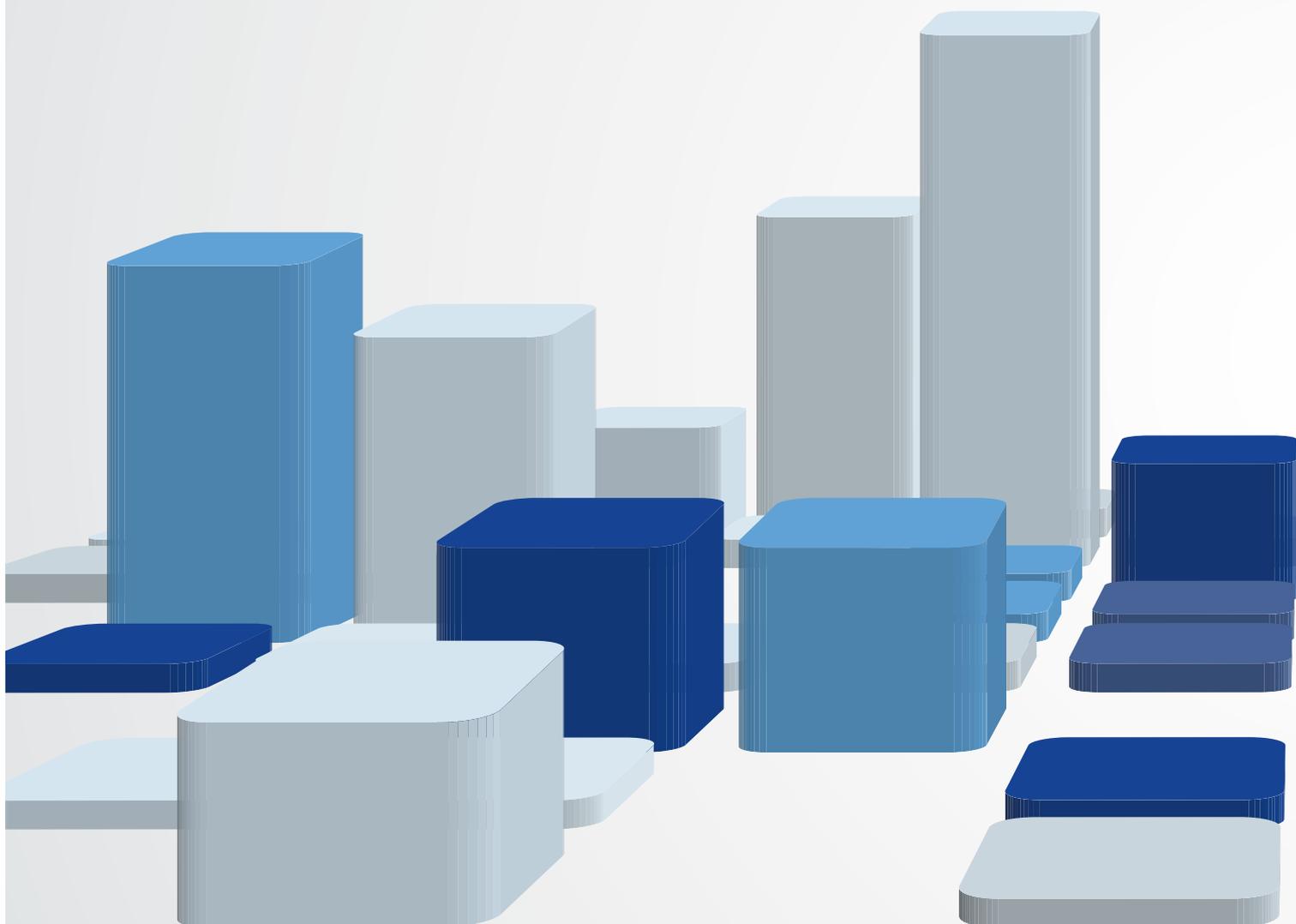
华为创造性地利用了IPv4报文头中至今唯一保留的bit位：Flags字段的第0位，用以对目标业务流进行染色。由于绝大多数利用IP通信的业务都要有标准的IP报文头，因此这种染色方法可不依赖于业务类型，方便设备进行硬件处理。

直接检测机制，故障检测精准

对业务流质量进行直接测量，无需插入测试流，检测路径与真实业务路径合一，故障精准定位到链路、板卡甚至芯片。

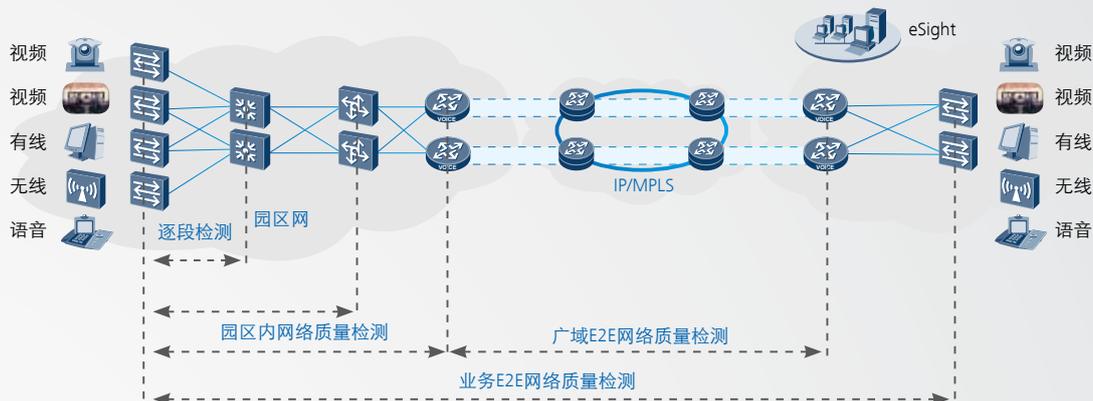
基于ENP以太网网络处理器，轻松实现对任意业务流进行检测

为了对目标业务流进行故障检测，需要对业务流进行区分和着色，传统的交换机只能用有限的ACL资源进行业务流识别，且只能用CPU对报文进行染色，性能低下，无法规模部署。而基于ENP的S12700敏捷交换机支持高达256K ACL，可对任意业务流进行标识，并且用微码来对业务流进行染色，实现线性转发。



iPCA应用场景

iPCA应用于多种场景，如园区、电力、IP RAN以及ISP链路租用等，通过对丢包、时延、抖动等网络质量的检测，迅速定位视频、语音、有线无线等应用的故障原因。



iPCA园区应用场景

如上图所示，iPCA可逐段检测接入、汇聚、核心乃至广域各段的网络指标。故障定界迅速精确，可立刻判断出故障发生在网络中的某一块板卡甚至某个芯片，为解决故障提供强有力的保证。即使在广域网部分不支持iPCA特性，通过对广域两端的园区出口进行分析，亦可确认故障是否发生在广域部分，明确责任归属。End

自在融合，一统有无

——华为校园网U²M统一用户管理新方案

文/夏阳松

校园网需要精细化管理

《国家中长期教育改革和发展规划纲要（2010年—2020年）》明确要求“要提高国家财政性教育经费支出占国内生产总值比例（GDP）的4%”；另据计世资讯（CCW Research）研究表明，2012年中国教育行业IT投资总规模为439.1亿元，同比增长达20.9%。随着教育体制改革的深入和教育信息化进程的不断推进，高等教



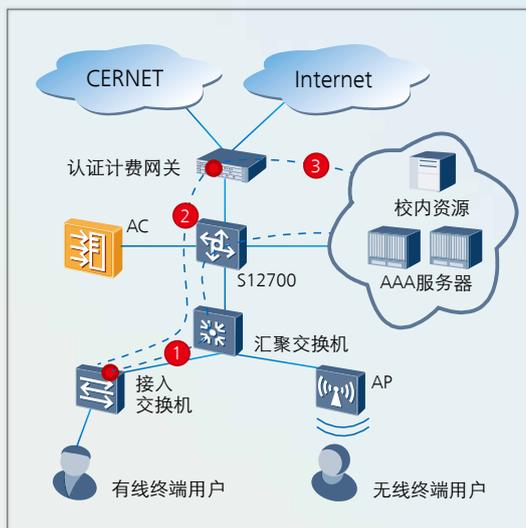
育、基础教育、职业教育、特殊教育的信息化都得到了不同程度的发展。

目前，校园网的主要诉求集中在以下几点：
设备投资要集约、网络运营要自主、无线接入要全覆盖和用户管理要完善。

其中，对用户进行精细化管理是目前园区网建设过程中存在的核心诉求之一。针对这种核心诉求，目前有两种传统的解决方案：基于准入准入出两次认证的用户管理和以独立BRAS为核心的用户管理。前者对交换机要求低，但管理能力有限；后者可对用户精细管理，但需要购置昂贵的独立BRAS。

传统用户管理解决方案概览

方案一：基于两次认证的用户管理

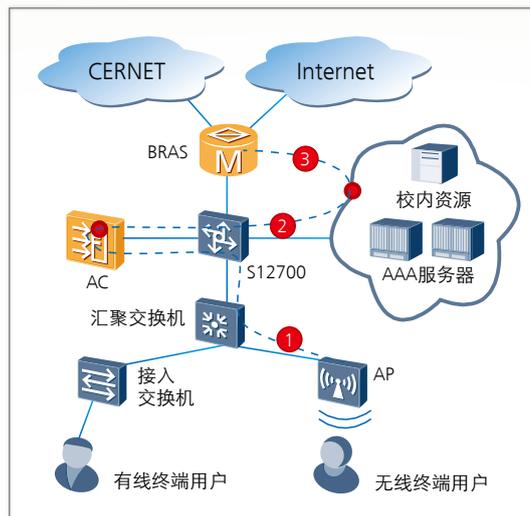
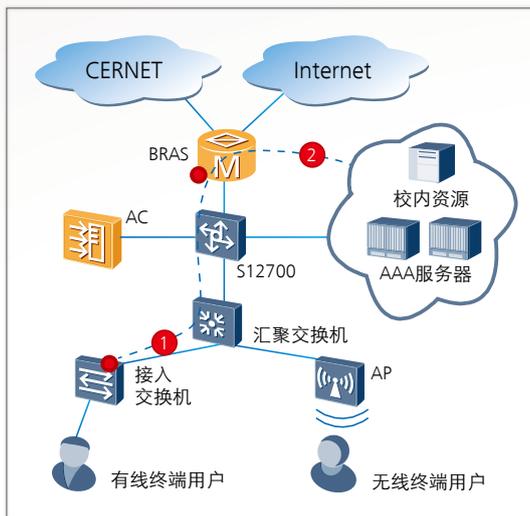


如上图所示，接入交换机和认证计费网关分别控制着对校内资源和校外资源的访问。这里以有线终端用户为例（无线用户则需通过AC来做校园准入认证）。首先，有线终端用户通过802.1x客户端进行第一次身份认证，即校园网准入认证；接入交换机作为RADIUS客户端，与AAA认证服务器进行交互；认证通过后，接入交换机将接入用户与MAC、IP、物理端口进行绑定，确保合法用户可以自由访问校内资源。其次，当用户访问校园外部资源时，认证计费网关需要对用户进行第二次认证，也即准入认证。最后，当用户通过准入认证后，AAA服务器将该用户的授权信息下发到认证计费网关，启动计费，并对用户的上网行为进行监控。

这种方案技术实现简单，但缺陷也很明显：认证点繁多，有线用户通过接入交换机认证，而无线用户又集中到AC认证；策略管理复杂，全靠ACL来限制用户的互访和权限，一个中型网络需要配置数千条，大型网络则需配置上万条，且ACL部署在不同的节点，超级复杂。



方案二：以独立BRAS为中心的用户管理



BRAS因其成功在运营商网络部署而被引入到校园网。BRAS具有强大的认证计费功能：PPPoE认证、IPoE+QinQ认证、802.1x认证、Portal认证、按流量计费、按时长计费、预付费、套餐计费、计费保护、不计费等等。如上图所示，对于有线终端用户，首先，接入交换机为每个用户分配一个VLAN，对接入用户进行流量隔离，确保没有通过认证的用户不能进行互访。从技术上来看，接入交换机对用户流量封装了第一层Tag，汇聚交换机对用户流量封装了第二层Tag（QinQ），BRAS通过QinQ封装的PPPoE/IPoE协议对终端用户进行认证。然后，BRAS利用RADIUS协议向AAA服务器发出认证请求，认证通过后，AAA服务器对BRAS

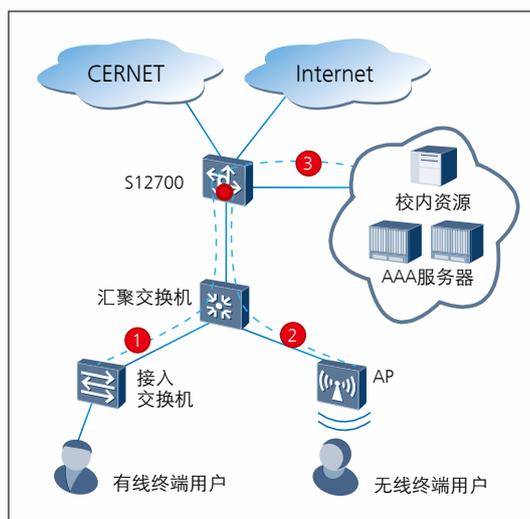
进行授权，启动计费，进而实现了准入准出一次认证，内网外网统一监控。对于无线终端用户，如上图所示，AC对移动终端进行认证；认证通过后，AAA服务器对AC进行准入授权，并将授权信息下发给BRAS，进行准出授权，做到“一次认证，两面授权”。

由于利用了专用的用户管理设备BRAS，该方案具有集中认证、策略管理简单等优点，但其不足之处也是显而易见的：需要单独购买BRAS设备，价格不菲；AC和BRAS是两个不同的物理设备，联动困难；用户认证流程复杂，无法对有线用户和无线用户进行统一管理。





华为U²M统一用户管理方案



集采众长之下，华为创造性地推出了以S12700敏捷交换机为核心的U²M（Unified User Management）统一用户管理方案：随板实现了BRAS特性，有线无线统一认证；每个用户都有单独的用户表，用以实现对用户的权限、带宽和QoS控制。华为U²M方案的推出，最终实现了园区网络从“以设备管理为中心”到“以用户管理为中心”的飞跃。

如左图所示，首先，有线终端用户的接入认证报文通过接入交换机，透传到核心交换机。然后，无线终端用户的接入认证报文通过AP的CAPWAP隧道封装，透传到核心交换机。最后，具有内置BRAS、内置AC功能的核心交换机将用户的认证信息传送给AAA服务器；认证通过后，AAA服务器通过核心交换机对用户进行授权、计费、行为监控。

相比传统的用户管理方式，此方案具有如下显著特点：

业界独创的集成随板BRAS和AC功能

以S12700为核心的精细化用户管理方案，内置了BRAS用户管理能力和AC功能，用户无需购买独立的BRAS、AC设备或AC板卡，就可实现有线无线用户的统一管理。既简化了网络部署，又节约了投资，同时支持IPv4/IPv6。

一致性体验，差异化服务

用户无论是以iPhone、iPad、Andriod终端等无线方式，还是以PC、视频终端等有线方式接入

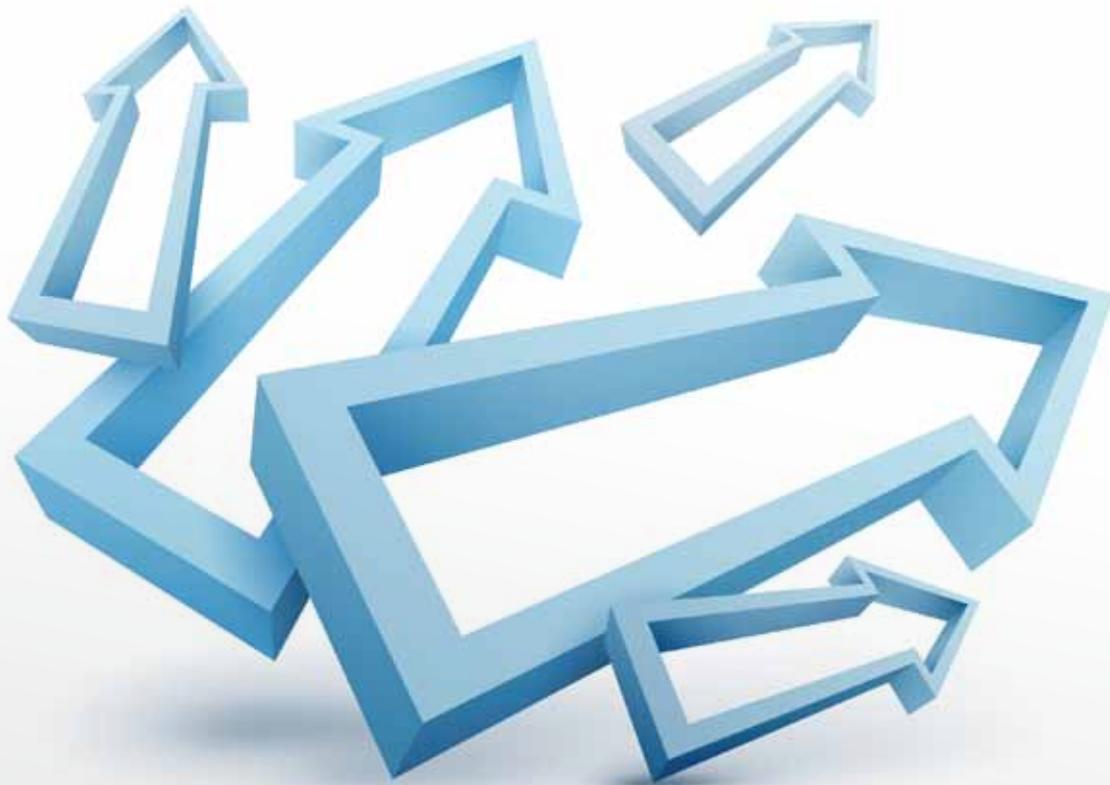
到网络，S12700都有能力提供一致的用户体验；另一方面，S12700支持完善的5级HQoS调度，可为不同客户和业务提供差异化服务，真正实现了“有线/无线同账号、内网/外网不同速、IPv4/IPv6不同价”的目标。

集中认证，接入层天然隔离

有线无线统一集中到内置的BRAS上认证，屏蔽了接入层设备能力和接入方式的差异；同时支持多种类型的认证方式，如PPPoE/802.1X/ MAC/ Portal /IPoE等等，可针对不同区域、不同运维要求，采用不同的认证方式，实现差异化管控。比如，在宿舍区，为防止学生进行网络攻击，可采用PPPoE管道化认证；在教师办公区，为简化认证过程、避免安装PPPoE客户端，可采用IPoE+QinQ方案；而对于一些办公设备，如打印机，则只要进行最简单的基于MAC的认证即可。

策略管理简化，取消用户控制ACL配置

传统园区网本质上是“以设备管理为中心”，如果要对用户（而不是端口）进行带宽管理、权限控制，只能利用交换机上非常有限的ACL资源来实现。而S12700采用了以“用户管理为中心”的设计理念，每个用户都有单独的用户表，用以实现对用户的权限、带宽和QoS控制，可以做到分组、分域、分时对用户进行授权，8Kbps粒度的上下行带宽控制。基于简单灵活的策略管理，S12700更可按照不同的时间段、不同的业务类型、不同的访问地址等，进行差异化计费。另外，结合用户当前的位置信息，可以有效地进行安全策略联动，提高安全性。例如，相比于宿舍区，同一用户在实验室就可访问更多的教学资源。





为什么是华为？

所谓十年磨一剑。为什么是华为能够创造性地推出U²M方案？

深厚的交换和WLAN技术积累：华为具有成熟的交换机以及WLAN平台，其交换机和WLAN位列国际权威分析机构Gartner 魔力四象限中的”挑战者象限”，得到市场的广泛认可；

领先的BRAS技术能力：华为具有业界领先的BRAS解决方案，ME60产品连续多年占据市场第一；

强大的芯片研发能力：华为具有深厚的芯片研发能力，S12700是基于华为自研ENP芯片，既能像ASIC那样进行线速转发并保持低功耗，同时又提供了灵活的可编程能力。



深刻的行业理解：华为长期致力于提供卓越的校园网解决方案，为中国教育信息化打造定制化、本地化的强大网络。

技术上顶天，市场上落地。技术实力的积累和深刻的行业理解相结合，使得华为能够创造性地推出U²M方案，实现园区网络从“以设备管理为中心”到“以用户管理为中心”的飞跃。 **End**



敏捷交换机开辟 未来城域网建设新通路

文/王波

虚拟化、云计算、物联网等技术的成熟，将带来城域承载网络的革命性变化，向敏捷、动态、更可靠的云级以太网演进，是城域网的发展趋势。而城域网作为城市信息化建设的基础平台，包括政府、教育、广电等领域，都迫切需要构建超宽带、低成本、电信级、绿色环保、可以面向未来长期演进的全业务城域网，动态、敏捷地满足未来业务发展需求。但是，传统交换机无法从根本上满足城域网的要求。如何解决这个瓶颈？

为什么传统交换机无法满足城域网的要求？

从四个方面来讲，传统交换机对于支撑面向未来的、可演进的城域网显得力不从心。

1、城域网设备对路由能力的要求

当前Internet中实际运行BGP-4的骨干路由器的路由表已达到500K，对城域网建网设备的路由规格和转发性能提出了很高的要求。传统三层交换机由于采用ASIC芯片，在路由规格和转发性能上都受制于芯片设计，FIB表项至多仅为512K，每千条路由收敛时间高达30秒，路由能力无法满足城域网要求。

2、城域网设备对缓存能力的要求

由于城域网的网络流量规模非常大，且在业务高峰期会出现瞬时突发流量，因此城域网对网络的时延、丢包有非常苛刻的要求。基于ASIC芯片的交换机每块业务板卡缓存一般仅有4M，在局域网环境应用尚可，但在流量规模庞大的城域网环境下，则无法在网络突发流量时保证视频等实时业务不受影响。

3、城域网设备对网络服务质量的要求

随着高清视频点播、电子商务、云计算、物联网、远程教育和远程会议等网络应用方式的爆炸式增长，城域网的用户规模也在不断增长，需

要网络设备能够提供区分用户和业务的能力，以获得更好的服务质量。传统的QoS基于端口进行流量调度，单个端口只能区分业务优先级，无法区分用户和业务，成为进一步提高网络服务质量的瓶颈；而H-QoS既能为高级用户提供精细化的网络服务，又能从整体上满足不同用户群的网络体验，是构建城域网必备的技术需求。传统三层交换机由于ASIC芯片限制无法支持H-QoS，无法保证城域网的服务质量要求。

4、城域网设备对可靠性的要求

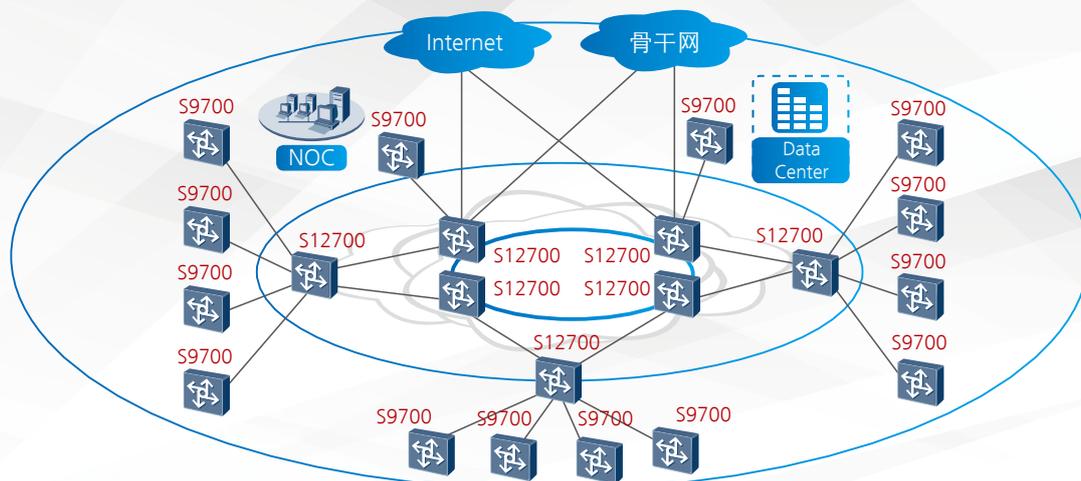
传统交换机由于采用ASIC芯片，路由规格和转发性能都受到芯片设计的限制，无法满足不间断路由、快速重路由和路由快速收敛等要求，甚至导致业务中断。

基于敏捷交换机构建可演进城域网

作为全球领先的信息与通信解决方案供应商，华为通过在数据通信领域的持续积累，推出性能卓越的S12700敏捷交换机，可以充分满足下一代城域网的建网要求。

基于敏捷交换机构建可长期演进的城域网弹性架构

考虑到未来的业务发展，基于MPLS的VPN技术是当前唯一能提供大规模、全互联、高速通信的技术，MPLS技术在骨干网、城域网、移动回程



基于敏捷交换机的城域网架构

网络中已经被大量使用，被证明是成熟可靠且扩展性良好的承载技术。S12700敏捷交换机支持完备的MPLS方案，可以满足拓扑结构庞大、节点错综复杂的城域网建网要求，并且随着新业务应用类型的增加，网络拓扑结构可动态增长。

敏捷交换机具备超大规格应用表项

S12700敏捷交换机的FIB表项高达3M，收敛时间达到6K/s，可媲美专业路由器的性能水平，真正实现了交换路由一体化，不仅能满足城域网网络拓扑庞大和业务复杂的要求，而且能满足未来业务发展的网络架构升级和扩容，可面向未来长期演进。

敏捷交换机具备超大芯片内置缓存

基于华为ENP技术，敏捷交换机S12700具备超大芯片内置缓存，每块业务板卡缓存容量高达1.5G，确保在城域网环境中网络流量突发时视频等实时业务不受影响，不会出现时延和丢包。

完善QoS机制提升城域网的服务质量

S12700敏捷交换机支持5级H-QoS，具备完善的网络资源分配能力，针对Triple play业务，提供了HSI、VOIP、IPTV等多业务QoS调度能力，真正实现业务服务质量的保证，不仅能为高优先级业务与应用确保带宽，还能与其他级别的业务之间共享任何限制的带宽，为高级用户提供精细化的网

络服务，提高网络利用率和效率，满足不同用户群的网络体验。

丰富的可靠性技术保障城域网稳若磐石

在设备级，S12700支持业界唯一的CSS2交换网硬件集群技术，区别于传统的业务板间通过光纤或电缆互联实现的业务口集群。该技术是基于核心路由器平台的交换网集群技术，集群设备间的报文交换无需经过业务板卡，直接由交换网间的硬件通道互联，省去了中间的多个故障易发生点，也减少了软件失效风险。在网络级，S12700利用ENP以太网网络处理器件发送业界最短时间间隔的3.3ms以太OAM探测报文，结合SEP、G.8032等环网保护机制，做到整网50ms故障倒换。

一张网络统一承载所有业务

基于敏捷交换机构建可长期演进的城域网解决方案，可广泛应用在政府、教育、广电等领域。在政府领域，可用于建设电子政务城域网，作为城域范围内各政府部门信息共享和交互的平台，偏远乡镇可以通过专线接入；在教育领域，该方案可用于建设教育城域网，市内的教育城域网可和区县学校的校园网络互联；同时，由于IP城域网对各类型业务的兼容性和扩展性支持非常好，该方案也可用于广电系统的模拟/数字电视节目传送，免除了对SDH/MSTP等传输网络的依赖，真正在一张网络上实现所有业务的统一承载。End

华为视频监控网络护航平安城市

文/赵兢兢

2013年4月15日，美国波士顿马拉松竞赛终点线附近陆续发生两起爆炸，造成3人死亡，170多人受伤。美国波士顿警方19日晚证实，一名爆炸案嫌疑人已落网，另一嫌疑人在与警方的交火中被击毙。短短四天，这起爆炸案件便已告破，而在整个历程中，视频监控技术起到了极其关键的作用。

根据Frost & Sullivan的一份报告，在2016年之前，网络视频监控市场将以每年复合增长率16%的递增速度快速发展。其中，亚太地区增长比率最为迅速，主要是由于中国、澳大利亚、新加坡等国家宣布了一系列针对安全基础设施发展的方案。从欧洲来看，城市IP网络监控系统成长强劲。

城市视频监控系统通过对街道、公共场所、交通工具等进行持续监控记录，在预防和减少犯罪行为上起到了非常重要的作用，同时也可作为甄别犯罪行为提供最为直接的证据。国内从2004年开始在多个示范城市开展平安城市建设工作，全国主要城市也从2010年开始大规模部署城市治安视频监控系统。



随着平安城市、平安校园等安防项目在全国范围的深入开展，机场、地铁、电力等用户对于视频监控覆盖范围、监控点数以及网络传输等要求的不断提升，具备布控区域广、无缝扩展能力强以及可组成复杂监控网络等功能的IP网络监控正在逐渐成为中国视频监控市场重要的拉动因素。网络视频监控整体解决方案，正在得到越来越多用户的了解和认可。

视频监控业务对网络提出了新的挑战

视频监控技术，随着计算机、编解码、网络传输技术的发展，经历了三个阶段的飞跃发展，目前正朝着数字化、智能化、IP化、网络化继续发展。同时，视频监控同其他技术相结合，产生了许多新的应用，在各行各业起着举足轻重的作用。智能化视频监控系统具备传统监控系统所不具备的特性：高清视频监控、行为模式分析、智能搜索等等，可统一管理数十万个甚至上百万个前端摄像头，视频监控业务对承载网络提出了新的挑战：

大带宽、高密接入：随着视频监控在各领域发挥越来越重要的作用，高质量监控视频越来越普及。高质量视频意味着高清、高码流，从而产生海量数据，对网络带宽要求较高。根据建设经验，为了进行监控覆盖，一个中等规模城市约需要36,000个监控摄像头，以预留20%端口做中短期扩容计，则需要43,200个接入端口，总带宽需求为 $36,000 \times 8\text{Mbps (高清)} / 40\% \text{负载} = 720\text{Gbps}$ 。

QoS：视频监控应用相比其他业务具有更高的QoS需求，如实时监控视频，对网络的性能和QoS要求更高：网络时延上限值为400ms，时延抖动上限值为50ms，丢包率上限值为 1×10^{-3} 。

高可靠：由于不间断监控的需要，视频监控应用对网络可靠性要求很高，如监控网络出现中断，则会造成关键数据丢失，以致无法取证等严重后果。因此，视频监控网络设备可靠性需达到99.99%，确保网络无单点故障，业务不中断。

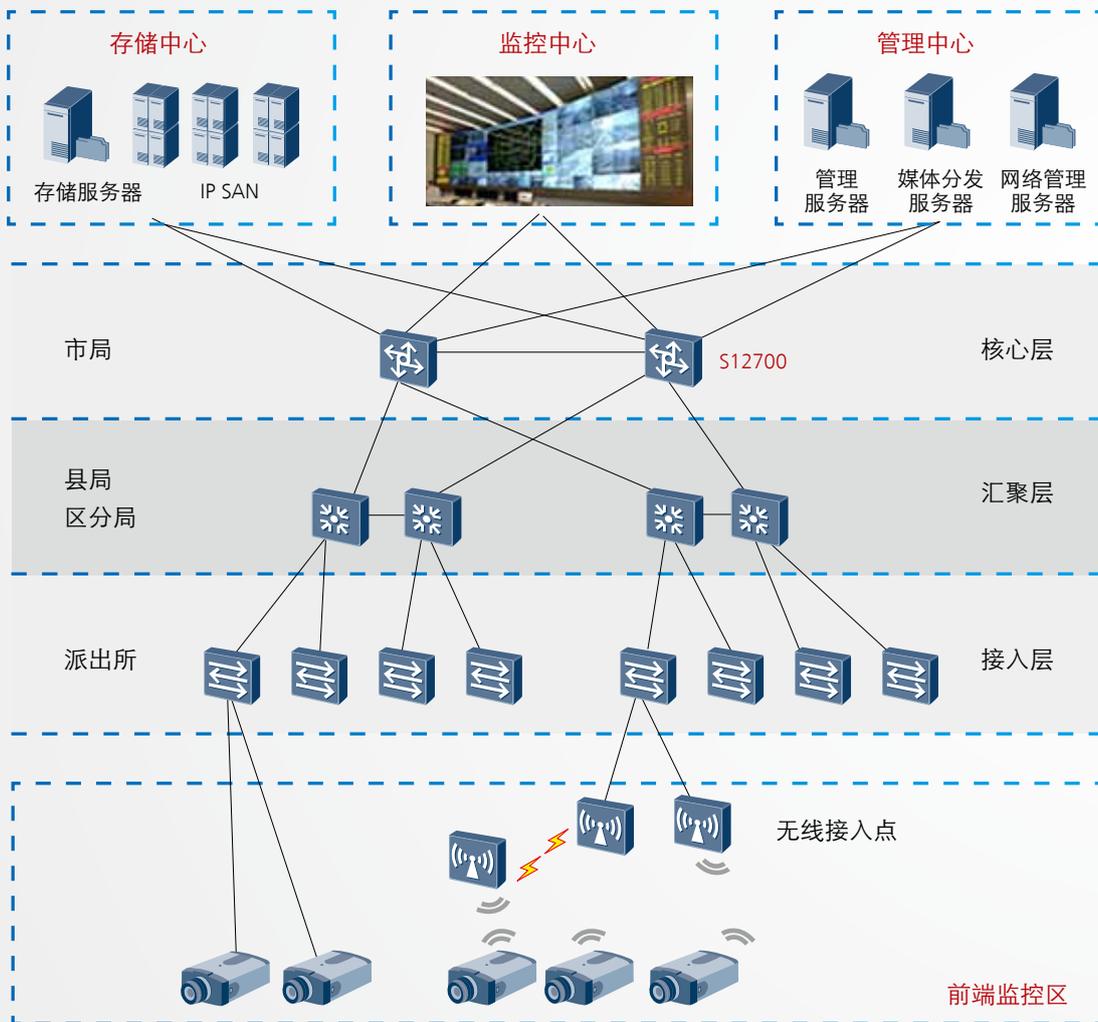
摄像头灵活接入：视频监控业务经常部署在道路、郊区等边远地带，存在取电困难、有线回传困难等部署问题。这样就要求视频监控网络具有灵活的摄像头接入能力，要求接入交换机支持PoE供电，以及AP能提供无线回传能力。

易运维：视频监控网络的不断部署和扩展，网络层次比较复杂，节点众多，带来巨大的网络运维成本。所以一张面向未来的视频监控网络应具有自动配置、智能化网络质量评估、智能故障上报等能力，从而简化网络管理，方便故障定位。



华为视频监控承载网络解决方案

典型的视频监控方案包括视频存储中心、业务管理中心、视频监控中心、前端监控区等四个部分，这四个部分通过IP承载网络进行互联。如下图所示：



华为视频监控承载方案具备以下特点：

大带宽、高密接入

作为视频监控网络的核心，华为S12700敏捷交换机支持高密10GE、40GE、100GE端口，而多台S12700可以组成CSS2交换网硬件集群系统，应对大流量对网络核心带来的巨大挑战。与此同时，华为具有丰富的二三层接入交换机款型，可满足百兆、千兆、光、电等各种接入场景需求。

完善的QoS保障

由于网络具有收敛性，视频监控对承载网络核心提出了更高的要求。S12700敏捷交换机支持5级H-QoS，对流量进行精细化区分、调度，确保高级别流量优先通过。S12700的核心是ENP以太网网络处理器，该芯片可外挂的1.5G DDR内存用于报文缓存，确保视频传输可靠、流畅。

端到端硬件保护

华为推出了业界唯一的从设备级到网络级的端到端硬件保护倒换方案，确保视频监控承载网万无一失。在设备级，S12700在继承了核心路由器平台技术的基础上，利用华为独创的CSS2交换网硬件集群技术，将多台设备虚拟成一台，集群

设备间的报文交换直接由交换网间的硬件通道来完成，省去了中间的多个故障易发生点，确保核心节点万无一失；在网络级，S12700利用专用硬件发送业界最短时间间隔的3.3ms以太OAM探测报文，结合SEP、G.8032等环网保护机制，做到整网50ms故障倒换。

灵活的摄像头接入方式

视频监控常常部署在广场、街道、郊区等有线部署困难、取电困难的区域，华为视频承载网络解决方案集成了无线接入、大功率PoE供电、太阳能供电等技术，提供了灵活的前端监控摄像头接入方式。而基于华为高性能AP的无线WIFI回传方案，部署便捷，建网周期短，可扩展性强，可大大降低接入网络的部署成本。

智能网络，简化管理

华为全系列交换机可支持Easy Operation功能，从Easy Install（易安装）、Easy configure（易配置）、Easy monitor（易监控）、Easy Trouble Shooting（易排障）四个方面，确保接入交换机全免管理，简化网络运营维护。

从以前的模拟监控到现在的数字监控；从落后的现场监控到先进的远程监控；从简单录像显示到智能化预警；从有线到无线，视频监控技术正发生着具有深远意义的变化。华为视频监控网络解决方案，是华为基于对视频监控网络持续深入研究的成果，可满足视频监控网络高传输质量、高可靠、灵活接入等特殊需求，是为视频监控业务量身打造的新一代解决方案。End



华为S12700， 高品质VOD网络的巅峰之选

文/魏良浩

高清数字机顶盒的普及带来了VOD视频点播业务的飞速发展，截止2012年底，我国数字机顶盒市场装机容量已经突破1亿台，据预测，2013~2017年年均数字机顶盒的装机容量约为4000万台/年。VOD业务的发展对城域网带宽、时延和可靠性都提出了更高的要求，但是现有的骨干汇聚IP网络却无法满足不同VOD业务的快速增长。

另一方面，成为一个以高清视频为主要业务，同时提供宽带上网、多媒体通信、大客户VPN以及企业专线等多业务融合的运营商已经是广电运营商的重要诉求和发展规划。作为广电运营商，应该如何升级现有的网络，才能满足VOD的发展需要呢？答案就是构筑大缓存、高可靠、高智能的业务承载网。

VOD对承载网提出的三点诉求

诉求一：大带宽高可靠网络

VOD用户快速增长，随之而来的是网络带宽的快速扩容，从省干到地市再到县市级接入，均需要数倍甚至10倍以上的带宽增长才能满足巨量的VOD高清视频流。部署在各节点的网络设备必须具备强大的数据处理与转发能力，才能将VOD内容高效地分发到下级网络。

大流量的数据处理与承载，对处于核心或汇聚位置上的设备要求很高，若出现故障则会牵一发而动全身地影响整网运作，因此高可靠性设计必不可少，设备倒换不能影响到开展中的业务。

诉求二：突发流量轻松应对

相对于单向的电视节目收看而言，VOD用户访问网络的内容随机性和时间集中性的特点更为突出，对网络的冲击也是显而易见的。比如，在周末节假日或者是平日的黄金时段，VOD视频总

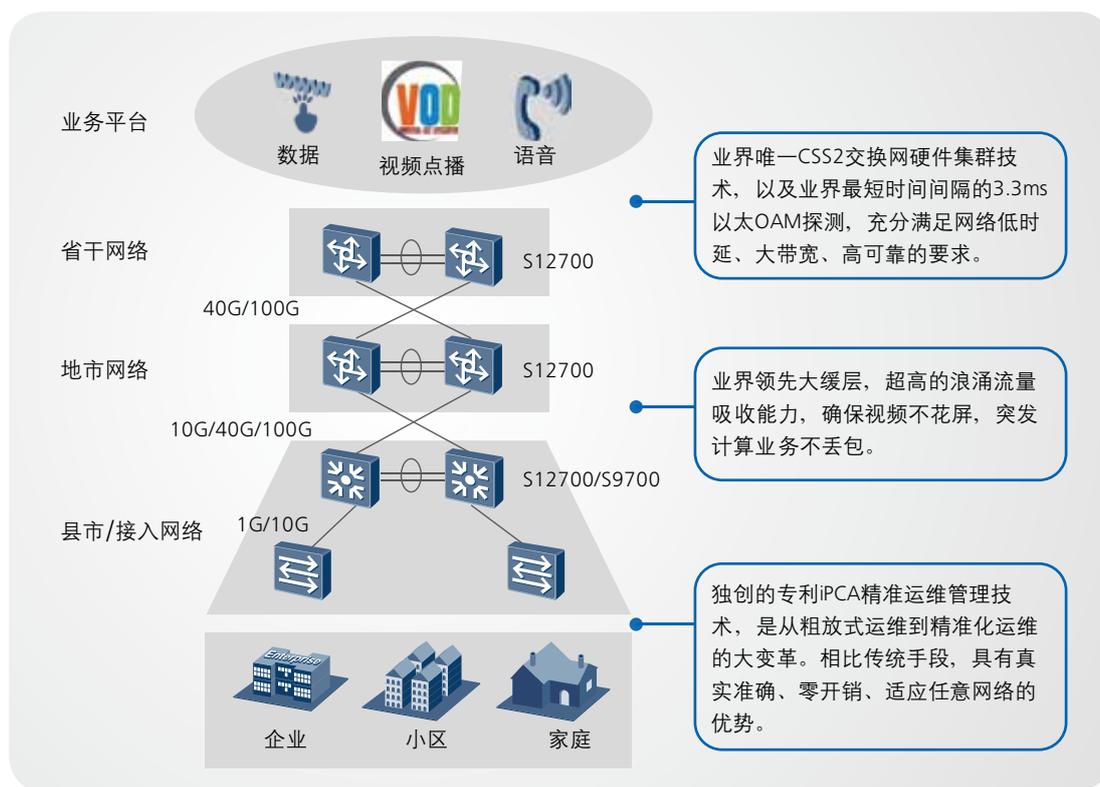
流量会因为点播的用户增多而暴增，再加上用户点播动作的随机性导致的突发流量，很可能导致网络来不及处理突发而出现丢包。

诉求三：网络质量监控平台

高清互动VOD业务对网络提出了更高的要求，最终反映的是终端用户的切实体验和感受。仅停留在常规网络KPI的运营维护已经不能满足用户要求，广电运营商必须要掌握用户真实的业务体验与网络运行状态，要能够判断VOD业务的质量，准确检测每个用户的网络承载情况，并能快速定位故障及可能存在故障隐患的网络节点。

基于华为S12700构建下一代VOD网络

S12700敏捷交换机，是华为新一代的高端交换机，支持CSS2硬件集群技术、大缓存技术和iPCA（Packet Conservation Algorithm for Internet）网络包守恒算法，完美地满足了VOD业务的网络需求。



业界唯一：从设备级到网络级的端到端硬件保护倒换

在设备级，S12700支持业界唯一的CSS2交换网硬件集群技术，区别于传统的业务板间通过光纤或电缆互联实现的业务口集群。该技术是基于核心路由器平台的交换网集群技术，集群设备间的报文交换无需经过业务板卡，直接由交换网间的硬件通道互联，省去了中间的多个故障易发生点，也减少了软件失效风险；并且由于跨框报文一次转发，较传统业务口集群的多次转发大大降低了时延。在网络级，S12700利用ENP以太网网络处理器发送业界最短时间间隔的3.3ms以太OAM探测报文，结合SEP、G.8032等环网保护机制，做到整网50ms故障倒换。

业界领先：大缓层、超高浪涌流量吸收能力

视频流特别是高清视频流具有带宽大、丢包敏感的特点，在VOD系统里，视频流更具有显著的突发特征。传统基于商用ASIC芯片的交换机一般每

板只有4M缓存，无法对视频突发流量进行有效的吸收，导致花屏、不清晰。S12700敏捷交换机基于ENP芯片技术，通过芯片外挂DDR内存，实现了每块业务板内置1.5G缓存，确保视频传输可靠、流畅。

业界独创：iPCA网络包守恒算法，助力网络精准化运营

凭借对IP网络及运维的深刻理解和二十多年的研发积累，通过对网络、标准、协议等的深入探索研究，华为发明了一种IP网络性能直接测量算法：iPCA网络包守恒算法。传统的检测手段（如NQA、Y.1731）通过仿真流或模拟流来推测网络质量，测量精度差；而iPCA是一种随路精准检测技术，通过对业务流进行标识、染色和计数，让用户之间的数据流在传送业务的同时，也具备网络质量检测功能，解决了IP网络故障检测的业界难题。基于ENP以太网网络处理器的S12700运用了这一独创的专利技术进行精准运维管理，实现了从粗放式运维到精准化运维的大变革。End

如何实现无线园区 网络精准规划？

文/丁秋方

BYOD和移动办公已经是大势所趋，也顺势掀起了一股去有线化浪潮，自然而然地，WLAN在网络接入方面将扮演越来越重要的角色，而网络规模大、接入复杂、用户流动频繁的园区网，WLAN的覆盖必将越来越大。如何快速、方便地规划并构建高质量WLAN网络，成为无线园区网络建设的迫切需求。

目前业界流行的规划方案都需要通过手工绘制墙体等障碍物信息，缺乏总体的3D建筑物模型。华为继承了在3G无线领域10多年的技术和经验积累，将先进的3G网络规划理念、方案和经验数据应用到WLAN上，推出了以“WLAN Planner”和“WLAN Survey”工具为核心的无线园区WLAN规划方案，形成了“自动识别障碍物”，“一体化工勘”以及“自动生成3D建筑模型”的完整解决方案，可快速、轻松、准确地完成WLAN规划，让用户在规划阶段就能看到网络部署以后的结果，使得园区网在规划初期就具备敏捷基因。



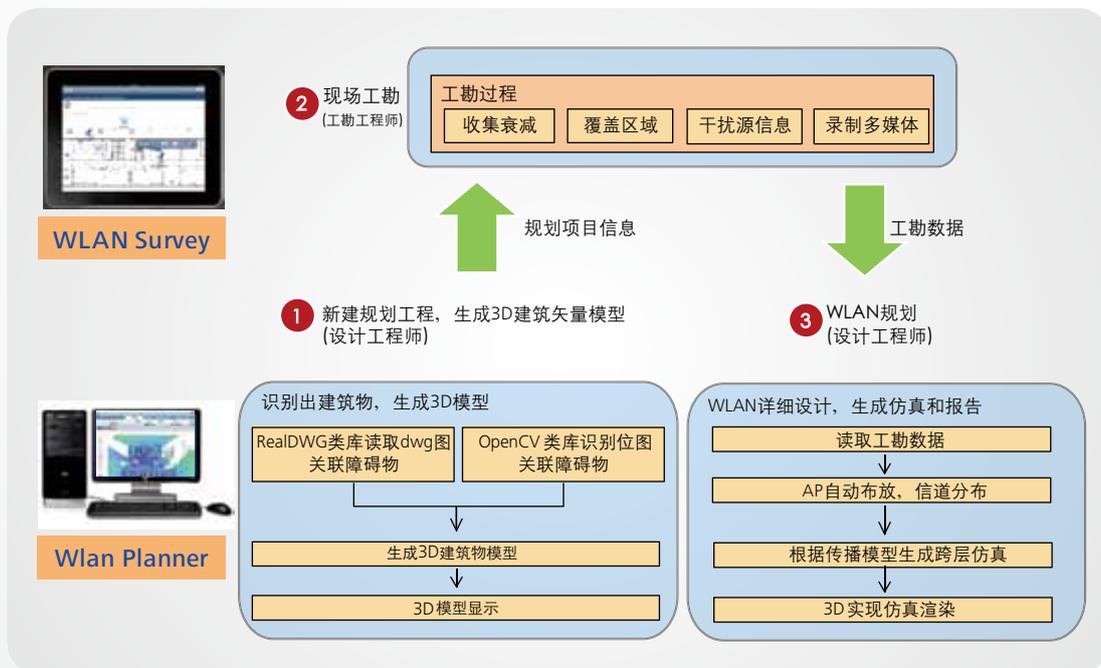
为什么要做WLAN网络规划

WLAN网络的开放基因决定了其网络质量容易受到蓝牙、微波炉、无线摄像头等设备干扰。在传统有线网络，提高网络容量最常用的办法就是增加设备。但是，在WLAN无线网络中，针对同一信道的不同设备，只能有一个处于数据传输状态。所以在WLAN中，越多的设备加入，设备之间冲突越大，网络容量越低。众所周知，WLAN频谱资源稀缺，不重叠信道数量很少，2.4G频段有3个不重叠信道，5G频段具有的信道稍微多一些，不同地区情况不同，为了提升网络容量，必须对网络进行精确规划，使WLAN总体性能最佳。

另外，WLAN部署环境复杂。WLAN信号是一种电磁波，电磁波在传播过程容易受环境的影响。其在穿透墙体等介质时，信号强度会根据材质和厚度有不同程度的衰减。为了精确模拟出WLAN设备与其他设备之间的干扰情况，就需要模拟出WLAN运行的实际环境，然后进行网络规划。而实际上，WLAN网络部署场景复杂多样，比如一栋大楼内，有砖墙、水泥墙、门、有色玻璃、石膏板和金属天花等不同的建筑材质，这些材质对WLAN信号造成的衰减不一样，不同厚度的材质对WLAN信号造成的衰减也不一样。

华为无线园区精准网规方案六大特色

在WLAN网络规划中，华为延续了在无线领域十余年的网络规划经验，设计出“准备——概要设计——工勘——详细设计”的标准流程，针对上面三个诉求进行重点攻克，推出了WLAN Planner和WLAN Survey工具，形成了“自动识别障碍物”，“一体化工勘”以及“自动生成3D建筑模型”的完整解决方案，可快速、轻松、准确地完成WLAN规划。



WLAN规划的全流程图

准备和概要设计阶段：根据用户提供的建筑图纸信息（包含CAD、PDF和普通位图），模拟出客户现场的3D环境；并根据图纸中墙体、门窗的固有特征，把障碍物分成不同的类别，默认关联成砖墙、承重墙、承重柱、门和窗等类别，同时自动把经验库中的衰减值关联。特别值得一提的是，该工具会把图纸中开发式的门变成闭合的门，能够更真实地模拟现场情况。

工勘阶段：WLAN Survey工具，是一款安装在Android平台的智能终端软件，可方便地把WLAN Planner的规划结果带到工勘现场，进行有针对性的工勘。该工具把现场弱电房、干扰源以及其他典型的特点记录下来，确认图纸的比例尺信息，

记录楼层属性，提供衰减测试、记录干扰源等功能，极大地提高了工勘的效率，降低了出错的可能性。

详细设计阶段：依赖在华为3G无线网络的经验积累，并根据WLAN的实际测试，得出不同场景下的信号强度传播模型公式、信干噪比模拟公式和吞吐率模拟公式。结合逼真的3D环境和工勘的实际数据，输出精确的3D仿真。这种所见即所得的效果，让用户在规划阶段即可知道部署以后网络的性能。

独有的射频模型

基于在无线特别是3G领域十多年的宝贵经验，华为通过大规模的WLAN实验测试，充分考虑传播过程中信号的反射与衍射，针对开放空间、半开放办公区和景观隧道等不同场景，固化了信号强度传播模拟公式、信干噪比模拟公式和吞吐率模拟公式。结合精确的3D模型，华为公司不仅考虑水平方面的信号影响情况，还考虑了垂直方面信号的互相影响，使得规划结果更加精准。

完备的经验数据

华为的规划工具具有自动识别障碍物的能力，相比手工绘制建筑信息，不但效率更高，而且更加精确。可以区分成不同的墙体、门、窗

等，对于一些细节也都能准确无误地体现出来。对于不同的建筑材质可以做到区分，根据图纸中墙体、门窗的固有特征，把障碍物分成不同的类别，默认关联成砖墙、承重墙、承重柱、门和窗等类别，并自动把经验库中的衰减值得关联，可以精确绘制建筑的3D模型，准确地模拟出客户现场的情况。

便捷的工堪工具

智能终端越来越普及，WLAN Survey工具可以安装在普通的Android无线终端上，无需专用的工堪终端就可便捷地将工堪现场的结果带到规划现场，确保规划准确，有针对性。End



基于SDN架构的 下一代敏捷园区网

文/姬亚南

园区网挑战

企业园区网承载的业务正在发生变化，从数据业务、少量语音以及视频业务，向云计算、移动办公、社交媒体、以及大量语音视频等实时业务转变。业务的快速变化，对现有的网络带来诸多挑战：

1、移动办公带来的挑战：静态 VS 动态

面向用户的策略管理，是网络能够更好的保证业务安全和体验的核心要素。目前很多企业的策略管理都是采用人工静态配置方式，企业网络全球化之后，员工经常需要异地办公，安全以及QOS策略需要能够跟随用户迁移至本地进行部署，采用人工静态配置的方式不仅工作量大，而且无法快速响应用户需求。移动办公的一致性体验是另外一个棘手问题，员工出差到异地，经常面临数据访问网络延时大，语音效果不好等问题，办公效率大打折扣。

2、网络安全带来的挑战：单点静态防御 VS 多点动态未知威胁

基于各种安全考虑，企业会部署防火墙、IPS、DLP等多种安全设备进行防护，但各司其职，彼此之间基本无交互，属于单点静态防御。企业面临的安全问题是什么情况呢？a) 安全边界模糊化：BYOD导

致终端安全和信息安全问题激增；企业全球化使网络边界模糊； b) 攻击手段多样化：据Gartner统计，75%的威胁发生在应用层，>50%攻击是有组织的团队行为 c) 从已知威胁到未知威胁：攻击转向使用未知威胁变种，以躲避传统防护手段，仅中国，2010年新增网络病毒1798万。网络的安全威胁无处不在，攻击复杂多变，安全需要全网协同防护。

3、网络运维人员面临的挑战：状态不可知和管理不自动 VS 新兴业务和海量设备

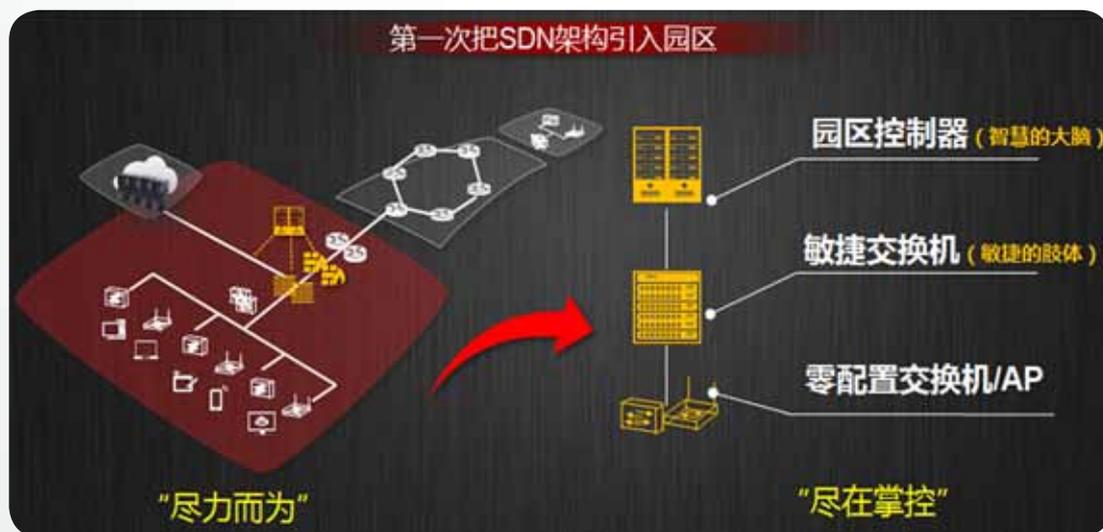
运维挑战来源于两方面：一是针对业务质量的快速感知和定位问题。企业新增的视频、桌面云等大多是实时业务，对网络质量敏感，如视频要求丢包率<10⁻⁶，语音<10⁻²。目前网络针对用户感受到的，如马赛克、听不清等问题，却并不感知，直到被员工投诉，更痛心的是在被告知问题之后也没有有效的手段快速解决。另外就是海量设备部署管理问题，包括众多接入层设备部署带来巨大的手工静态配置工作量，以及有线网、无线网等多种网络缺乏统一管理。

4、新兴多业务带来的挑战：僵化的网络 VS 多变的业务

新兴业务快速发展，对应的各种协议、标准层出不穷，从IETF RFC的数量上就可以看出端倪，数量从80年代的几百篇，在2009年达到将近7000篇。目前一个新兴业务如果采用租用方式部署，几天即可上线，而新设备的开发至少要1年，芯片开发至少要2年，传统网络已经无法快速适应业务的更新换代。

基于SDN架构的下一代敏捷园区网

园区网络急需一场架构变革来快速匹配业务发展，华为依赖敏捷交换机和园区控制器，第一次把SDN架构引入园区。首先，给网络增加了智慧的大脑——园区网控制器，实现了全网统一的协同控制和策略管理。其次，通过敏捷交换机为网络提供了敏捷的肢体，能够实现对策略的敏捷感知和执行。最后，大量的接入设备，如交换机和AP等可以做到零配置上线，极大简化网络的配置和管理。借助全新的网络架构，同时推出“业务随行、安全协同、业务感知和管理、有线无线深度融合、全可编程网络”五大创新方案，让网络更敏捷地为业务服务。



创新一：业务随行

第一个以业务体验为中心的网络方案。园区网控制器向运维人员提供面向业务诉求的策略配置，如用户组属性、QOS等策略。用户在任意地点接入，控制器感知用户接入位置，自动下发策略到对应的网络控制点（汇聚交换机、出口路由器等），进行安全控制以及QOS调度，实现策略

随行。同时，后续还会考虑和数据中心控制器进行联动，把用户的业务资源（存储，桌面云VM）跟随用户终端的接入位置，迁移到最近的数据中心，实现资源随动和体验随身。

动态工作组，基于身份动态创建虚拟工作组，千里之外如一间办公室。企业基于安全需要，通常会考虑按照部门或业务划分隔离区，对于大型园区每一次的业务重新隔离和网络调整都涉及到数以万计的配置策略调整，非常难以维护并容易出错。华为园区网控制能够提供的基于工作组的横向，以及纵向互访策略配置，在用户接入后自动下发和执行，创建一张无处不在的虚拟网络。

创新二：安全协同，实现分布式动态感知、全网主动防御

园区网控制器在策略控制的基础上，集成了



安全日志管理中心，依赖高效的大数据分析及事件关联能力，能够对全网的安全事件进行协同分析，准确识别潜在的安全威胁，同时能够和用户安全策略控制联动，实现就近阻断。如安全日志管理中心在明确某用户的DDOS攻击后，自动将安全准入策略在接入层下发，对用户进行隔离或者直接下线处理。

控制器还能够根据用户属性，定义不信任流量策略，如访客等，自动将流量引入安全中心进行流量清洗，防止潜在的威胁，实现主动防御。

创新三：业务感知和管理，第一次让IP感知质量

传统的网络质量检测方法，如NQA、Y.1731等技术需要另外插入检测报文，或者存在报文乱序等问题，其网络检测的精准度不足一半，而且此类技术存在监控对象单一、适用场景有限、受网络类型限制等等问题。经过多年的技术研究，华为公司业内首创研发出了网络包守恒算法iPCA(Packet Conservation Algorithm for Internet)，第一次为传统网络增加了一个主动质量感知机制，实现了即时质量感知和即时故障定位，从根本上攻克了IP网络的体验保证难题。iPCA技术通过对业务流进行标识、染色，在出口和入口同时对染色包做检测，从而检测出网络的丢包、时延、抖动等质量参数。该技术让用户之间的数据流在传送业务的同时，也具备网络质量检测的能力：与传统网络质量检测方法相比，iPCA技术具有如下优点：1) 0流量开销 2) 适用基于IP的任意网络类型（单播，组播），任意网络规模 3) 精确到设备内部（单板）级的精确故障定位。

创新四：有线无线深度融合

无线网络有线化。敏捷交换机通过独有的可编程能力，实现了CAPWAP隧道终结等传统AC功能集成，直接对AP进行管理和流量转发。以此为基础，在管理界面上，还能够将AP虚拟成交换机一个端口，实现“有线网络+无线网络=一台交换机”，极大的降低了WLAN网络部署后对运维人员的技能要求。

有线网络无线化。敏捷交换机基于CAPWAP隧道，用管理无线AP的同样机制管理接入交换机，实现“接入交换机=AP，汇聚交换机=AC”，接入交换机部署将类似AP的免配置开局，降低海量接入层设备的部署工作量。

创新五：全可编程网络，平滑演进

基于ASIC的交换机针对新兴业务要求过于僵化，为避免频繁的替换网络，保护用户投资，华为基于敏捷交换机的新一代园区网提供全面的可编程能力，在现有网络上平滑升级：

POF支持未来协议可编程：基于华为独有的可编程交换机POF协议无关转发（Protocol Oblivious Forwarding）技术，网络行为完全由控制面负责，企业可以自定义策略实现新业务报文识别，针对新兴业务适配不需改动已经建设好的物理网络，更好的保护企业用户的已有网络投资。

芯片支持转发平面可编程：前述方案中提到的有线无线融合，iPCA业务质量感知方案都已经用到了敏捷交换机的转发面编程能力，而这可能仅是冰山一角。面向未来的多样业务，可编程的转发面将会有更多的使用场景，比如hybrid openflow流表转发的支持等。

架构支持多层次开放：整个SDN方案架构，不仅支持转发面编程，控制器本身也提供了开放的API供业务系统使用，比如用户信息的同步，网络质量监控数据的获取等。

结束语

基于SDN架构的下一代敏捷园区网从网络基础机制上消除了传统网络缺乏体验保证，部署低效和响应慢的问题。从业务被动适应网络，转变为网络主动适应业务，从而构建一个业务友好的网络。同时，通过可平滑演进的SDN架构，优先解决用户现网问题，并能演进至未来网络，让网络更敏捷地为业务服务！ **End**



版权所有 © 华为技术有限公司 2013。保留一切权利。

非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。

商标声明

 HUAWEI、华为、 是华为技术有限公司的商标或者注册商标。

在本手册中以及本手册描述的产品中，出现的其他商标、产品名称、服务名称以及公司名称，由其各自的所有人拥有。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文当信息仅供参考，不构成任何要约或承诺。华为可能不经通知修改上述信息，恕不另行通知。

华为技术有限公司
深圳市龙岗区坂田华为基地
邮编：518129
电话：+86 755 28780808

www.huawei.com