DOI: 10.3969/j.issn.1009-6868.2015.06.012
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20151105.1923.006.html

M-ICT时代下的全面扁平化趋势

The Trend towards Flatness in M-ICT

王德政/WANG Dezheng
王承忠/WANG Chengzhong
吉晓威/JI Xiaowei
(中兴通讯股份有限公司中心研究院,深圳 518057)
(Central Research Institute of ZTE Corporation, Shenzhen 518057, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2015) 06-0049-005

摘要: 在M-ICT时代,物理设备、网络部署、业务流程都呈现全面扁平化的趋势。在物理设备层面,各类资源的池化已成为主要趋势;在网络部署层面,软件定义网络(SDN)/网络功能虚拟化(NFV)等技术令网络部署更加趋于扁平;在业务流程层面,大数据系统为扁平化提供了技术基础。指出安全问题泛在化与安全边界模糊化是扁平化趋势带来的新安全课题,在安全架构的构建中,需要重点考虑这两方面的问题。强调M-ICT时代将是一个全面扁平化的时代。

关键词: 扁平化; 资源池; 大数据; 安全

Abstract: In the M-ICT era, the trend of flatness is evident in physical equipment, network deployment, and business processes. At the physical equipment level, pools of all kinds of resources have become the main trend. In the network deployment level, software-defined networking (SDN), network function virtualization (NFV), and other technologies can make the network flatter. In the business process level, big-data system provides the technical basis for flatness. We point out that the safely problem become general and security boundaries become blurred. We need to pay attention to these two aspects. We emphasize that the M-ICT era will be a comprehensive flat era.

Key words: flatness; resource pool; big data; security

在互联网思潮的冲击下,网络扁平化趋势已成为业界共识。随着M-ICT时代的到来,扁平化已不仅仅停留在网络扁平化的层面,物理设备、网络部署、业务流程都有全面扁平化的趋势。这些“扁平化”技术将为管理扁平化趋势提供技术支撑,并将会全面提升M-ICT时代下的工作效率。

1 设备扁平化趋势

1.1 IT资源池化的趋势

在M-ICT时代,IT基础设施需要提供快速的业务部署能力和高效的设备运维能力,对物理设备也提出了更高的要求。

传统设备将从单个实物形态的设备逐步过渡到池化设备形态,即一个管理域内的数百乃至数万台物理设备组合成一台池化设备。池化设备具备业务所需的各种功能部件,不同的功能部件由不同的物理资源池提供,设备也从“黑盒”逐步过渡到“白盒”。整个网络和IT基础设施可认为是由少量扁平化的池化设备组合构成[1]。

在传统“烟囱式IT”向云计算基础架构演进的过程中,资源池概念逐步得到了丰富和发展。通过虚拟化的方式,服务器、存储、网络等资源全面形成一个巨大的资源池。通过分布式算法将这些资源进行分配,从而消除物理边界,提升资源利用率,最终实现按需动态分配资源。更进一步地,云计算技术将打破服务器机箱、机柜的限制,把所有的CPU和内存等资源解放出来,汇集到一起,形成CPU池、内存池、存储池以及网络池,当用户产生需求时,便从这个池中配置能够满足需求的组合。

对于计算资源和内存资源池化,因为受带宽和时延约束,当前CPU资源和内存资源,还属于紧耦合绑定状态,随着硅光互连技术的发展和成熟,未来有解耦成相互独立资源池的趋势。

对于存储资源池化,以存储区域网络(SAN)/网络连接存储(NAS)为代表的传统网络存储,已逐渐演变为不同SAN/NAS系统之间存储资源共享,并由此产生了基于虚拟化的存储资源池化。随着未来技术进步和需求驱动,接近内存性能的非易失性随机访问存储(NVRAM)、依赖总线和接口标准(PCIe)互连的非易失性存储器标准(NVMe)的固态硬盘(SSD)等新型存储介质也将得到商业应用。

网络资源池化是一个逐步发展和完善的过程。多台虚机共享物理

收稿日期:2015-09-10
网络出版时间:2015-11-05

网卡，每台虚机呈现“独立”的逻辑网卡，这属于网络资源池化概念雏形。未来网络的开放和可编程特性，使得网络资源对用户将呈现资源池化的特征，即实现网络资源的按需分配，满足资源池内设备互连以及外部互通等各种应用场景。

1.2 IT资源池化的关键技术

传统服务器的各个组成部件都是固定配置的，为了进一步提升资源的利用率、要求服务器的功能标准化，形成更多功能级的资源池，各个组成部件通过解构与重构，重新组合成逻辑设备单元。为了实现池化设备的解构与重构，需要解决IT系统内部的互连问题，同时需要一个高效的管理体系。我们将简要描述IT资源池化的一些关键技术。

1.2.1 池化设备解构与重构

首先，出于成本、节能减排的考虑，我们需要把电源、风扇部件从服务器基本构成中解构出来，使得多台服务器共享风扇、电源，这也是谷歌自研定制化机柜式服务器的初衷；其次，多服务器之间共享存储，共享网卡也是服务器解构的一种表现形式；最后，IT领域为了上层业务匹配最合适的服务器资源，一般把服务器的IO卡（网络）、内存条、硬盘设计成可配置方式，使得服务器可重构。

OCP、天蝎等开源组织更是大大推进了服务器解构与重构的进展，将其从手工方式提升到自动化规模部署。传统通信技术产业（CT）领域的电信设备一般是分布式部署，这些独立设备在引入池化概念后，将解构成不同的部件，并逻辑层面重构为逻辑单元。电信设备IT化已被全球电信运营商广泛接受，采用传统信息技术产业（IT）服务器承载电信业务已有许多成功案例。

1.2.2 池化设备的内部互连

池化设备的内部互连是指：从各种资源池中选择硬件模块，然后通过内部互连，构成逻辑设备。内部互连到底选择什么技术方案，一方面取决于该技术的服务质量（QoS）相关指标（带宽、时延、抖动等）是否满足应用需求，另一方面取决于该技术的产业成熟度和成本。

目前硬盘资源和服务器之间主要是通过串行连接SCSI（SAS）交换实现互连，而CPU资源与外部IO之间一般通过PCIe互连。随着技术进步，高速存储介质通过PCIe互连，所以在资源池化设备中，存储资源池将采用SAS交换和PCIe交换融合方案，统一提供低速或高速的存储介质。

目前以太网已成为设备内部或设备之间最主流的互连方式，随着云计算相关业务对高带宽低时延需求的广泛性，支持全称远程直接数据存取（RDMA）将成为以太网技术的基本选项。目前网卡共享主要体现在服务器内部多虚机之间，随着multi-host网卡技术的发展，多台服务器之间通过PCIe交换共享网卡，这将为云计算带来诸多优势。

随着芯片处理能力的逐年增强，芯片管脚数不能同步增加，电信号传输速率也受印刷电路板（PCB）的制约。硅光技术是解决上述问题的关键，硅光互连解决了芯片之间的互连带宽问题，配合全光背板和硅光交换机技术，可以在数据中心范围实现资源池的全光互连。硅光互连将成为池化设备内部的主流方案，是未来主要方向。

1.2.3 池化设备的管理

池化设备管理主要采用RESTFUL接口，可以实现管理程序和设备之间解耦，便于各自升级扩展。

分布式管理任务组（DMTF）制订了相关协议，该协议包含交互协议和资源封装格式，资源的表现形式为协议无关的JSON/Odata格式。

服务器、机框、机架等各个层级的设备，通过支持统一的管理接口，实现资源池设备的扁平化管理。

2 网络部署扁平化趋势

网络扁平化主要指网络层次简单，业务部署简单，运维简单。

运营商网络基本形成了典型架构，它一般由接入网、汇聚网、核心网3个网络层次构成，同时，传输层面还有光网络/IP网络的层次结构，相互之间的业务互通主要通过配置方式，业务部署灵活性不够；另一方面，网络设备都是独立的“黑盒”设备，全分散的控制架构，使得整个网络的运维显得复杂、低效。

为促进网络的进一步扁平化，引入SDN架构显得非常重要；而NFV对电信业转型也起到关键作用，通过其灵活性、低成本、易拓展、快速应用开发等特征可以重塑传统电信网络和业务。SDN和NFV的结合给运营商网络部署提供了扁平化创新和变革的“引擎”。

2.1 SDN导致承载网络扁平化

SDN是网络演进的关键技术，它可以实现控制与转发分离的架构，逐步被IT和CT领域普遍接受。目前SDN场景也逐步从数据中心（DC）向运营商广域网（WAN）、移动网络（5G）扩展，进一步拓展到了池化设备内部网络的应用场景。

当前的承载网主要由底层的光网络和上层的IP网构成，基本上属于静态网络，可编程能力比较弱，对于复杂多变的流量模型调度手段少，响应缓慢。

在M-ICT时代，承载网引入SDN架构，实现转发和控制分离、控制面集中，并通过引入可编程环境实现网络的端到端全局资源调配能力，支持复杂多变的各类业务流量模型。

SDN对网络端到端能力的提升，将在以下几个方面有所体现：

（1）高效弹性部署，提高网络资源利用率。由于引入了一个集中的全局网络控制面，可以更有效地进行

全局网络视图规划，控制和管理，并通过软件编程实现部署自动化。

（2）端到端的业务体验。集中控制和统一策略部署能力使得端到端的业务保障成为可能，网络能力开放，网络可与上层应用更好地协调，物理网络和逻辑网络实时状态监控与协调，都保证了网络业务体验。

（3）简化网络，降低网络复杂度。通过采取软硬件解耦以及转发控制分离等技术，逐步实现网元设备池化，各功能部件独立发展，并最终实现全网简化，降低总拥有成本（TCO）。

SDN的引入，模糊化了传统承载网络与内部网络的边界，减少网络的层次，使承载网络更加扁平化，更容易适应端到端业务需求的变化。

2.2 NFV导致通信网元扁平化

在软交换技术时代，以话音业务为主的通信网首次引入承载与控制分离的概念，传统电路交换也由扁平化IP交换替代，话音通信网因此实现了第一次扁平化改造；在移动互联时代，话音和数据均是IP承载，扁平化趋势越来越明显：在2G、3G时代，网络层次从基站到控制器再到核心网，共3层；在4G时代，网络层次弱化了控制器，业务流实现了从基站直接到核心网的二层架构；在5G时代，5G网络架构将把基站和核心网网关集成在一起，将垂直的网络架构演进为水平的一层网络架构，网络层进一步扁平化。

NFV架构以云计算为基础，软硬件解耦，实现通信网的水平切割及业务的快速发布。在2G/3G/4G混合组网的场景下，通过引入NFV架构，可在一个公共的硬件资源池中实现网元虚拟化。即根据不同的用户比例及业务特点，灵活调整各虚拟网元的部署规模，实现网络与业务在整个演进过程中的最佳匹配。随着5G时代的到来，适当增加硬件资源池中转发功能部件，以及软件化基带处理部件，能够灵活构建全新的5G虚拟化网元。在整个通信网络扁平化演进过程中，NFV是核心支撑技术。同时，NFV支持通信网资源开放，给运营商的经营创新带来了机会。

3 业务流程扁平化趋势

3.1 大数据的智慧生成提供扁平化技术基础

无论是流程上的分层，还是管理上的分层，其原因之一是人类处理复杂信息能力的局限性，所以需要分层的流程与管理，并进行逐层信息收集、分析以及汇总。对于很多组织来说，中层领导的主要工作职责就是向上进行信息汇总以及决策建议，向下进行命令传达与执行。大数据技术第一次让人类具备处理海量信息，并直接从这些海量信息中生成智慧的能力。大数据的智慧生成的能力，为流程扁平化提供了技术基础。

大数据如何进行智慧生成呢？这需要从信息模型中进行分析。信息模型从底向上分为4个层次：数据、信息、知识和智慧。其中，单纯的数据本身并无实质性意义，信息是由数据加上内容定义而构成，知识是由信息加上规则而构成，最高层的智慧是由知识加上经验而构成。而提升人类活动准确性的工作，是由位于信息的最高层——智慧层来完成的[2]。

无论是对于人类自身，还是计算机系统来说，比较容易处理数据、信息、知识这3个层次的信息，因为其本质都是数据的存储与检索，只是人类的处理效率与准确性要低于计算机。但是对于如何从知识中获取智慧，无论是人类还是计算机，都是一件非常困难的事情。

在大数据诞生以前，智慧很难通过机器得到。各个行业的智慧生成都是依赖各行业的专家，一个专家的能力是与他在行业内的经验积累密切相关的，其所沉淀积累的知识越多，则做出正确抉择的可能性越大。但人类专家的工作效率和准确性均有限，特别是在经验或数据缺乏的情况下，专家们往往依靠直觉做判断，并通过层层的流程与管理进行筛选与决策，加剧了结果的不准确性。

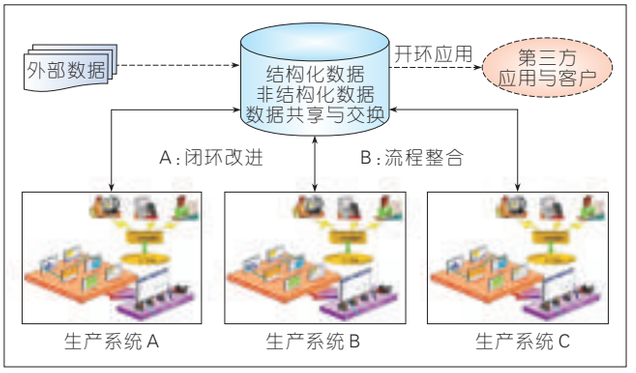
通过大数据的挖掘手段，可以依托海量的知识库，将输入的知识或信息转化为智慧。未来，机器可以通过海量数据挖掘、发现知识并输出智慧，再由人类专家对结果进行检验与校正，并通过机器学习，逐步提高结果的准确率。通过这样直接从海量信息中生成智慧的技术，让流程的扁平化具备技术可行性。

3.2 大数据的架构加速扁平化趋势

在过去的十年里，智能终端和移动互联网的快速发展深刻地影响和改变着人类社会。传统的“注意-兴趣-搜索-行动-分享”购买模式已经被打破，变得更为个性化。变化更快的市场环境使得现有的市场经营模式能够发挥的作用逐渐变小，企业越来越依赖数据分析指导自己的产品，改进服务，迎合市场需求。数据和数据处理能力成为企业在新的市场环境中生存、发展的关键。2014年，阿里巴巴集团创始人马云在互联网大会上说道：“人类正从IT时代走向DT时代”。

如图1所示，我们可以采用以数据为中心的系统架构，提高生产效率及反应速度，并满足客户个性化需求。大数据主要在3个方面促进业务流程扁平化。

（1）通过收集生产系统产生的业务过程数据，对业务数据进行建模，对当前生产系统提出建议与分析报告，从而去除或改进现有系统中不合理的环节，提高系统生产效率，降低成本。例如，通过收集无线网络的网络覆盖信息，可以对现网的网规、网优工作进行指导。与传统依靠路测进行网规、网优的模式相比，采用该种方式后无论是资金成本还是时间成本，都将急剧降低。



◀图1
大数据促进业务流程扁平化

（2）通过将生产系统中的数据进行集中汇总，并通过大数据的分析与挖掘，可以直接给出相关的经营与决策建议。与传统的层层上报、层层决策的模式相比，这将显著提高决策效率，加快市场反应速度，并减少决策失误。

（3）在多个生产系统需要协调配合时，可以通过集中的数据，在多个生产系统之上构建更高层面的无缝对接流程。与传统的人工流程对接相比，这将极大地提高系统之间的协调速度，并降低对接出错的概率。

4 扁平化趋势下的安全技术

4.1 安全问题特性

在M-ICT扁平化趋势下，安全问题呈现出泛在化与边界模糊化这两个显著的特征。

对于安全问题泛在化，呈现出新的特点。

（1）攻击源节点和目标节点泛在化。随着智能终端、物联网和云计算的发展，攻击源节点和目标节点已经不局限于原有的计算机系统和移动终端，摄像头、汽车、机顶盒、打印机、个人穿戴设备、智能医疗设备等都可能成为攻击的源节点或目标节点。这样使得攻击载体的规模迅速放大，物联网终端将成为高级持续性威胁（APT）攻击的跳板和僵尸网络的目标。统计数据表明70%的物联网终端存在安全漏洞，且缺乏认证和传输加密。

（2）攻击途径泛在化。在M-ICT时代，万物互联使得各种终端可通过Wi-Fi，zigbee，蓝牙等多种途径接入网络，相应的攻击途径也得到了扩展。并且，SDN架构、云计算架构下丰富的应用程序网络接口（API）也成为理想的攻击途径。

（3）攻击目的泛在化。首先，SDN和云计算本身带来了新的安全问题，例如，SDN控制器是网络的控制中枢，如果SDN控制器受到攻击可能导致整个网络瘫痪或者被劫持；例如，采用虚拟化技术的云计算，也会引起数据残留、资源风暴等新的安全问题。其次，物联网的兴起让攻击者的攻击目的从传统的网页漏洞与应用程序漏洞，转移成窃取智能联网装置的资料与控制权、破解车载系统漏洞、入侵医疗设备仪器等。攻击者只要能渗透智能终端、智能家具或者是智能联网装置，便能窃取机密资料、取得控制权，甚至劫持这些智能联网装置发动更大规模的攻击。

对于安全边界模糊化，其表现在网络边界的模糊导致原有安全边界的模糊。

首先，随着移动办公、BYOD等应用，处于企业外网的终端需要访问企业内网资源，突破了内外网隔离的边界。其次，云环境下多租户共用物理资源，多个租户的服务可能运行在一个计算节点上，租户间没有物理上的明确边界。再次，企业的Wi-Fi接入、咖啡馆热点接入、机场热点接入、家庭接入都存在众多的“最后一公里”网络，有众多的数据中心和应用程序网络接口，没有明确的安全边界，造成信任缺失。

安全问题泛在化与安全边界模糊化是扁平化趋势带来的新的安全课题，在安全架构的构建中，需要重点考虑这两方面的问题。

4.2 安全技术发展趋势

4.2.1 利用SDN架构特性解决安全问题

SDN本身会引入一些安全问题，但同时也可以借助SDN架构解决安全问题：

- SDN能够基于流模式提供端到端、面向业务的连接模型，并且不受到传统路由的约束，可以实现基于流的控制。
- 集中控制的特点有助于建立全网视野，可以在整网监控威胁。
- 安全策略的粒度管理可以基于应用、服务、组织、地域等，不取决于物理配置。
- 基于资源的安全策略可以紧凑地实现多种威胁的防御措施，增强管理。
- 通过编排可以动态、灵活地调整安全策略。
- 灵活的路径管理，快速封装以及隔离入侵可以不冲击到其他网络用户。

4.2.2 利用大数据特性解决安全问题

可以借助大数据的特性解决扁平化趋势下的安全问题：

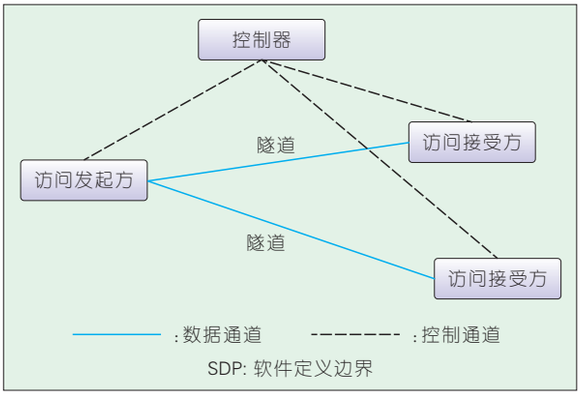
- 网络吞吐的倍增以及攻击的泛在化，导致攻击数据隐蔽在海量业务数据中，这极易触及安全设备的性能瓶颈，因此有必要引入大数据分析方法。
- 可以基于大数据分析方法进行安全管理平台（SOC）的海量系统日志分析，netflow/IPfix流量分析、安全策略分析、审计分析。
- 传统的安全防护手段如深度

包检测(DPI)、深度/动态流检测(DFI)、入侵检测系统(IDS)、入侵防御系统(IPS)、防病毒等都是基于特定规则进行匹配运算,符合大数据处理特性。

• 攻击手段的隐蔽化,尤其是APT攻击的发展,使得单个安全设备仅能获取部分攻击片段而防护失效,大数据技术可以汇总完整的攻击数据从而进行综合分析。

4.2.3 软件定义边界

如图2所示,软件定义边界(SDP)通过利用云计算,在任何IP可寻址实体间创建高度安全的、终端到终端网络,缓解可访问的互联网应用程序的风险,在连接网络前对设备和用户进行身份验证。



▲图2 SDP模型

SDP采用机密网络模型来保护应用程序,传统边界已经迅速成为设备在网络内部移动以及应用程序从网络边界迁移到云计算的障碍。通常在机密或高度安全网络,每台服务器被隐藏在远程接入网关后面,用户在查看和访问授权服务之前必须进行身份验证。

SDP保留了"需要知道"模型的优势,同时消除了对远程访问网关设备的缺点,SDP要求端点在获取对受保护的服务器的网络访问之前,必须进行身份验证以及获得授权,然后在请求系统和应用程序基础设施之间会实时创建加密连接。请求系统可以是移动设备,如智能手机、计算机或者传感器。

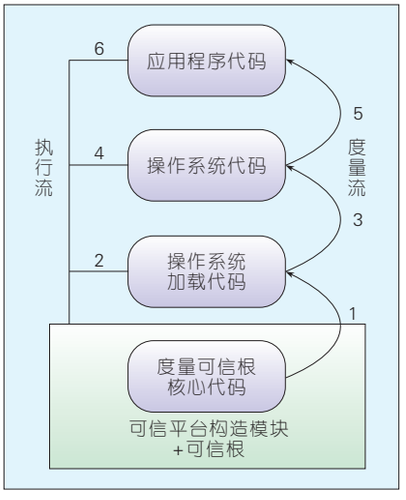
SDP采用了标准安全工具,如公钥基础设施、可信分层安全、IPsec和安全断言标记语言(SAML)以及地理位置等概念,来实现任何设备到任何基础设施的连接。SDP外围可以部署在任何位置,例如互联网、云计算中、托管中心、企业私有网络中,也可以跨网络部署。

4.2.4 构建可信体系

传统的安全解决思路立足于防,防火墙、IDS/IPS和AV构成了传统信息安全系统,并且以防外为重点,在物理边界上对非法用户和越权访问进行封堵,捕捉攻击和入侵的特征信息。由于其特征是已发生过的滞后信息,这样导致防总是落后于攻,也不能根据已有的可疑特征预测未来的攻击和入侵。

有别于传统的安全技术,可信体系的思路是消除恶意代码、病毒等攻击行为的作用空间。可信技术的根本机制如图3所示。

如图3所示,在系统启动过程中,有两个流按序串行进行:度量流和执行流。这两个流遵循先度量后执行的原则,保证了下一步执行的执行体是经过严格度量的可信任实体。



▲图3 可信体系的启动机制

可信体系由可信计算、可信存储、可信网络组成,并且在单个系统启动过程中进行逐级验证,形成网络中一个可信节点,与其他可信节点之间形成一个可信网络,从根本上提高整个系统的安全性。其中可信存储框架由TCG/T10/T13定义。

5 结束语

当前,对于物理设备、网络部署以及流程管理的扁平化,无论是理念还是技术,都已经具备实现的可行性。未来,M-ICT时代将是一个全面扁平化的时代,是一个端到端效率极大提升的时代。

参考文献

[1] 腾讯云:服务器资源池化技术发展趋势[EB/OL].http://www.cctime.com/html/2015-4-22/20154221716419323.htm

[2] Software Defined Perimeter Working Group. SDP Specification 1.0[S]

作者简介

王德政,中兴通讯中心研究院大数据首席架构师;长期从事中兴通讯大数据平台的系统架构设计工作;其参与研发的"多功能媒体网关"、"新一代集中网络管理调度平台技术创新及产业化"曾先后两次获得深圳市科技成果奖。

王承忠,中兴通讯中心研究院CSN分中心总工、系统架构师,中兴通讯技术专家委员会专家;长期从事通信设备以及ICT融合平台的研发工作;参与研发的"多功能媒体网关"获得了深圳科技成果奖,"ATCA高性能平台的产业应用"获得了南京市科学技术进步奖。

吉晓威,中兴通讯股份有限公司安全研究所总工程师;长期从事数据网络设备、通信系统设备研发工作,研究方向包括网络、安全、云计算及虚拟化等。