思科新一代数据中心架构—ASAP — 在线研讨会		
2017年3月2日		
序号	**问题**	**回答**
1	架构设计在软件层面和硬件层面不同的侧重点分别在哪些方面?	目前看来，软件和硬件（以硬件设备为基础的）架构设计基本的目标和衡量标准是趋同的。需要反映不同部门的需求，以及在应对变化和确保整体稳定性两方面保持适度的平衡。侧重点的分别，主要体现在组件的生命周期不同。软件的版本生命周期最短的可以以小时计；硬件的迭代周期则以月（增加新设备）至1~2年（研发周期）计，在线设备生命周期一般按5年估算（折旧）。所以在架构设计方面需要考虑这个差异性。 而这并不说明硬件比软件差，相对来说，硬件的性能和稳定性更好。同时，需要了解到，一些重要的、普遍采用的功能可能会在软件上先实现，之后成为硬件的一个功能。比如：虚拟化能力。 另外，FPGA的再次兴起，对于结合软硬件的优势可能会是一个重要的技术发展方向。但目前还有待观察。
2	现在我们的NEXUS能支持哪些第三方控制器？	本人并不了解是否有第三方的通用的商用控制器可以控制Nexus。而基于Open Daylight开发的控制器是有的，另外看到过有报道基于ONOS的开发的控制器也可以控制Nexus交换机，但不能确证。

3	现在传统的大型金融企业，网络，系统，应用 是分开管理，如何推进ASAP架构??	ASAP架构并不严格规定具体的实现形式，有很多设计的组合都可以进行，演进的方式也可以有多种。 对于不同部门分工比较明确的IT组织，基本建议是两个方面： 1.从组织架构层面重新思考进行组织功能和流程的整合，实际的案例告诉我们，进行“云”转型的IT组织，这几乎是必须要经历的过程，当然，这需要时间； 2.由发起项目的部门在组织范围内先引入新的架构，比如：ASAP，其他部门可以参考和学习这些新的架构思路和经验。通常会发起这些创新的部门可能会是，应用、虚拟化和网络部门。 特别需要理解的是，ASAP不仅是技术架构，更多的是架构的思维和文化问题。相信提问的朋友也注意到了这一点。
4	请问: 思科新一代数据中心架构在数据安全访问有何特点?	在新的数据中心架构中，安全是内生的，并且和其他功能是直接联动的——通过自动化和统一策略。这里统一策略指的是包含安全在内的多种策略的集合，策略的定义和引用可以是在整个IT系统内（或子集）内有效的，而策略的执行是自动化的。其次，思科的企业网架构DNA与ACI可以在策略层面进行集成，以实现从终端到服务器端策略的打通。 ——“数据的安全访问”，如果从基础设施层面大概可以这样理解。 如果问题是关于“信息安全”那应该是另一个问题，它与业务逻辑和用户鉴权认证等等相关，情况非常复杂，这里不做进一步解释了。

5	云计算的数据计算与分析属于大数据，传感设备必须使用N9000系列的吗？还有安全方面，硬件在进行大数据计算的时候，占用大量宽带资源与硬件设备性能资源，安全设备的安全策略是不是就无法做到很高的安全策略了。	第一个问题，推测是关于Tetration Analytics平台的，传感器可以是新的NEXUS 9000系列产品（当前发售的主流型号），也可以是安装在操作系统或Hypervisor一级的“软”传感器的实现。采用这两类传感器，实际效果差异并不大。差别在于，硬传感器可以捕捉交换机的运行数据（如：丢包，队列等），软传感器可以获取OS一级的额外信息，如：操作系统版本，PID等。 第二个问题，大数据应用的场景有很多，一般来说，基本的包过滤工作在NEXUS 9000上处理时没有性能方面的损耗。如果是复杂的状态检查或深度包检测相关的处理需要在专门的安全设备上进行——实际上，大数据平台通常在平台内是没有相关的复杂安全处理设计的，而在大数据平台对外的访问接口侧可能会有这样的要求，但流量很小，对通常的安全设备（如：防火墙）不会成为一个负担。
6	Cisco Tetration Analytics是有具体的产品么？	关于Tetration Analytis产品。请访问这里：http://www.cisco.com/c/zh_cn/products/data-center-analytics/tetration-analytics/index.html
7	请问硬件监控不采用镜像，采用的何种方式捕获数据？	在NEXUS 9000交换机上，数据包处理与捕捉回传都在同一个芯片上并行进行，所以不需要额外的镜像。
8	那旧的交换机需要能升级吗？	支持Tetration Analytics的传感器功能的交换机已经发售超过半年时间了，具体型号请参见http://www.cisco.com/c/zh_cn/products/data-center-analytics/tetration-analytics/index.html。 --“Cisco Nexus 92160YC-X 和 Nexus 9300-EX交换机具有内置硬件传感器”。如果比这些型号更早的话，对于固定配置的交换机需要替换支持，如果是机箱式交换机可以通过升级部分模块来支持。

9	請問，Tetration 從交換機送資料到分析後台時,這會對頻寬影響多少？	對頻寬的影響，在實際應用中觀察到的情況，一般不超過1%。原因是，資料傳送到後台前，會經過壓縮，并通過增量回傳的方式進行，而且回傳的是數據包頭部分，不包含全部業務數據，因此，頻寬遠遠小於原始的業務數據頻寬。
10	请问下老师，数据中心的安全需要怎么设计	安全的设计，这个题目范围太大了……。关于ASAP架构的安全保护的简要说明请见 问题5的回复。如需要进一步的讨论，请与思科相关区域或行业客户团队或AS团队咨询；或请本活动的负责人代转。
11	我们现在使用的是Cisco Nexus 7010交换机，无法支持ACI，现在遇到的问题是云环境无法满足网络安全分区的要求，用户申请的虚拟机访问DB 等其它资源时网络权限ACL 需要另外申请，严重影响了资源提供的时间。Cisco公司除了ACI 这样的SDN 解决方案外，针对Nexus 7000有什么好的解决方案，实现云计算环境满足网络安全域的部署要求？ 我们是2013年设计新数据中心的网络的，当时还没有流行SDN 概念，我记得在2014年才开始流行SDN 概念的。我们核心网络设备的老朽化周期为10年，刚使用3-4年的交换机，领导是绝度不允许更换交换机的。	应该是关于安全域部署的自动化方面的问题。基于Nexus 7000交换机，可以实现“可编程网络”或“可编程Fabric”这两种风格的设计或改造。“可编程网络”是通过RESTful接口或DevOps工具（如：Puppet、Ansible）来控制交换机实现自动化，需要有一定的软件或脚本开发工作。"可编程Fabric"也类似，但开发工作量会小得多。另外，有的企业会在现有数据中心先少量引入Nexus 9000和ACI，将自动化要求高（变更频繁）的业务先迁移到新的区域，再逐步扩大。 还有一种思路是，将不同安全域的虚机与网卡的子端口（VLAN ID）进行映射，同时在交换机上针对不同的子端口（预）配置不同的ACL。这种做法需要考虑一些技术细节问题，并进行整体规划。思路供参考。