网络虚拟化对数据中心的重要性分析思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_BD_91_E7_BB_9C_E8_99_9A_E6_c101_644041.htm 当下，在企业用户对应用整合需求越来越强烈的同时，对数据中心资源进行虚拟化整合也成为了一大发展趋势。网络虚拟化技术在数据中心资源整合过程中扮演着非常重要的角色，根据业务需求的不同，其形式也有所不同。 随着数据集中在企业信息化领域的展开，新一代企业级数据中心的建设成为了当前行业信息化的新热点。传统数据中心的关键需求是性能、安全以及业务连续性，然而随着企业应用的展开以及服务器、存储、网络设备在数据中心内的不断增长和集中，引发了新问题网络规划设计部门往往为单个或少数几个应用建设了独立的基础网络，这使得数据中心的网络系统十分复杂。正因如此，目前，在用户对应用整合需求越来越强烈的同时，对数据中心资源进行虚拟化整合也成为了一大发展趋势。 无疑，网络虚拟化技术在数据中心资源整合过程中扮演着非常重要的角色，根据业务需求的不同，其形式也有所不同: 如果多种应用承载在一张物理网络上，通过网络虚拟化分割(即纵向分割)功能可以使得企业内的不同部门或应用相互隔离，但同时可以在同一网络上访问各自不同应用，从而实现了将物理网络进行逻辑纵向分割，也就是说虚拟化出多个网络. 如果是多个网络节点承载上层应用，以往基于冗余的网络设计带来的是很高的复杂性，而将多个网络节点进行整合(即横向整合)，并虚拟化出一台逻辑设备，就可以提升数据中心网络的可用性以及节点性能，同时还简化了网络架构。 纵向分割 事实上，

网络虚拟化的概念并不是什么新概念，多年来，虚拟局域网(VLAN)技术作为基本的隔离技术已经被企业用户广泛应用。如果把企业网络分隔成多个不同的子网络，并且这些子网络遵循不同的使用规则，同时被分别控制，那么，用户就可以充分利用基础网络的虚拟化路由功能来实现隔离机制，而不再是依靠部署多套网络实现隔离。在交换网络上通过虚拟局域网技术来区分不同业务网段，同时配合防火墙等安全产品划分安全区域，本来就是数据中心建设过程中常用的方法。 现在，数据中心用户对于将多个逻辑网络进行隔离的需要越来越高。而VLAN、MPLS-VPN、Multi-VRF技术在路由环境下就可以实现对网络访问的隔离，并且虚拟化分割的逻辑网络内部有独立的数据通道，终端用户和上层应用不需要也不知道其他逻辑网络的存在。 当然，即便这样，在每个逻辑网络内部仍然存在着对安全控制的要求。尤其是对于数据中心而言，访问数据流从外部进入到数据中心，并且这些数据在不同安全等级的区域之间流转，因此，就更有必要在网络上提供逻辑网络内的安全策略。更何况，不同的逻辑网络对安全策略也有着各自独立的要求，这时就可以通过虚拟化技术将一台安全设备分割成若干台逻辑安全设备(成为多个实例)，从而更好地满足实施网络虚拟化后对安全控制的要求。基于纵向分割的网络虚拟化与虚拟化安全整合后的数据中心基础网络架构。 横向整合 数据中心是企业IT架构的核心之一，正因如此，用户在做服务器部署以及网络架构设计时，都是精细入微。由于多层结构、安全区域、安全等级、策略部署、路由控制、VLAN划分、二层环路、冗余设计等诸多因素，使得传统数据中心在网络架构设计上都是比较复杂的，

这就导致数据中心基础网络的运维和管理难度非常高。 这正是催生网络虚拟化技术在数据中心应用的重要原因之一。通过网络虚拟化技术，用户可以将多台设备连接，“ 横向整合 ”起来组成一个“ 联合设备 ”，并将这些设备看做单一设备对其进行管理和使用。多个盒式设备整合后类似于一台机架式设备，而多台框式设备的整合相当于增加了槽位。通过虚拟化整合后的设备组成了单一逻辑单元，在网络中表现为一个网元节点，这在让管理、配置、可跨设备链路聚合更简化的同时，还简化了网络架构，并进一步增强了冗余的可靠性。 此外，网络虚拟交换技术为数据中心建设提供了一个新标准，其定义了新一代网络架构，这样各种数据中心的基础网络都能够使用这一架构，这在帮助企业构建高效可用的状态化网络的同时，优化了网络资源的使用。同时，在网络虚拟化架构上，通过集成虚拟化安全，还可以使得传统网络中离散的安全控制点被整合进来。基于横向整合的网络虚拟化与虚拟化安全整合后的数据中心基础网络架构。 基于横向整合的数据中心网络架构与传统网络设计相比，有以下几大特点：运营管理简化。数据中心全局网络虚拟化能够提高运营效率，虚拟化的每一层交换机组被逻辑化为单一管理点，包括配置文件和单一网关IP地址。 整体无环设计。跨设备的链路聚合创建了简单的无环路拓扑结构，不再依靠生成树协议(STP)。虚拟交换组内部经由多个万兆互联，在总体设计方面提供了灵活部署的能力。 进一步提高了可靠性。虚拟化能够优化不间断通信，在一个虚拟交换机成员发生故障时，不再需要进行L2/L3重收敛，能快速实现确定性虚拟交换机的恢复。 安全整合。安全虚拟化在于将多个高性能安全节点虚拟

化为一个逻辑安全通道，安全节点之间实时同步状态化信息，从而在一个物理安全节点发生故障时另一个节点能够接管任务。 端到端的虚拟化 基于纵向分割和横向整合的网络虚拟化技术实现了对数据中心资源进行整合的目标，然而，更高层面的数据中心虚拟化技术带来的是对上层应用的灵活支持，并且会在很大程度上简化数据中心的运营。 数据中心内运行着企业的多种业务应用，计算层虚拟化技术让这些应用与具体物理服务器之间不再是完全固定的映射关系。可以说，计算资源池化(也就是服务器虚拟化)让数据中心实现了高密度，但同时，对于计算资源的动态调整就要求虚拟机可以在物理服务器之间迁移，并且还要求迁移网络是二层连接性的。 这时，为简化数据中心的二层互联设计，就可以通过网络虚拟化在更短时间内完成确定性L2链路恢复，同时不影响L3链路，这与传统的 MSTP VRRP设计有所不同。此外，虚拟化能够在网络各层横向扩展，这有利于数据中心规模的扩大，同时又不影响网络管理拓扑。基于虚拟化技术的二层网络在消除网络环路的同时，还有利于更大范围的虚拟机迁移。 业务连续性是企业IT运营的关键。目前，容灾、负载分担、保证业务连续性等都成为了企业构建新一代数据中心时的重要话题。集群互联是关键应用连续性设计的主要技术(服务器集群也是计算虚拟化技术)，目前在同一数据中心内实现集群并不是难事，一般的集群都是以二层连接为主的。但当业务连续性要求跨数据中心集群连接时，传统的网络技术支撑要做到可用性与可靠性，就会带来更高的复杂性，基于虚拟化网络的二层连接，可以将集群扩展到多个数据中心，从而带来应用设计上的灵活性。 对于企业而言，要应用访问控制，就

要对不同虚拟机实现隔离、对不同用户群实现隔离、对不同资源有独立的安全策略、对存储资源访问进行隔离、对异构存储通过虚拟化实现整合，并在客户端和数据中心形成虚拟化的资源分离通道。而要实现这些功能就要在用户接入层进行认证控制、在网络层进行虚拟化分离、在虚拟机之间隔离、将存储通道分离，并在不同资源类型之间增加公共标准化接口。实现了端到端虚拟化的数据中心网络架构。