解析虚拟化数据中心:网络虚拟化纵横谈思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/590/2021_2022__E8_A7_A3_E6_9E_90_E8_99_9A_E6_c101_590381.htm 随着数据集中在企业信息化领域的展开，企业级数据中心的建设当前成为行业信息化的新热点。传统的数据中心的关键需求是性能、安全、永续，随着应用的展开，服务器、存储、网络在数据中心内的不断增长、集中，引起较多的问题，网络规划设计部门往往为单个或少数几个应用建设独立的基础网络，使得数据中心网络系统十分复杂。 随着应用的整合需求越来越强烈，对数据中心的资源进行虚拟化是当前的主要趋势，也是当前IT业内最为令人关注的技术领域。 数据中心虚拟化的基础网络技术趋势，延续了传统数据中心性能、安全、永续的基本需求，而且进一步简化网络架构，更有力支撑应用层面虚拟化，降低运维复杂度，提高了灵活性。 网络虚拟化 网络虚拟化技术也随着数据中心业务要求有不同的形式。多种应用承载在一张物理网络上，通过网络虚拟化分割(称为纵向分割)功能使得不同企业机构相互隔离，但可在同一网络上访问自身应用，从而实现了将物理网络进行逻辑纵向分割虚拟化为多个网络.多个网络节点承载上层应用，基于冗余的网络设计带来复杂性，而将多个网络节点进行整合(称为横向整合)，虚拟化成一台逻辑设备，提升数据中心网络可用性、节点性能的同时将极大简化网络架构。 网络虚拟化---纵向分割 如果把一个企业网络分隔成多个不同的子网络——它们使用不同的规则和控制，用户就可以充分利用基础网络的虚拟化路由功能，而不是部署多套网络来实现这种隔离机制。 网络虚

拟化概念并不是什么新概念，因为多年来，虚拟局域网(VLAN)技术作为基本隔离技术已经广泛应用。当前在交换网络上通过VLAN来区分不同业务网段、配合防火墙等安全产品划分安全区域，是数据中心基本设计内容之一。 出于将多个逻辑网络隔离、整合的需要，VLAN、MPLS-VPN、Multi-VRF技术在路由环境下实现了网络访问的隔离，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均不会感知其它逻辑网络的存在。但在每个逻辑网络内部，仍然存在安全控制需求，对数据中心而言，访问数据流从外部进入数据中心，则表明了数据在不同安全等级的区域之间流转，因此，有必要在网络上提供逻辑网络内的安全策略，而不同逻辑网络的安全策略有各自独立的要求，虚拟化安全技术，将一台安全设备可分割成若干台逻辑安全设备(成为多个实例)，从而很好满足了虚拟化的深度强化安全要求。 如图1所示，虚拟化网络与虚拟化安全的整体结合，通道化设计，构成了完整的数据中心基础网络架构。 图1 基于纵向分割的网络虚拟化 网络虚拟化---横向整合 数据中心是企业IT架构的核心领域，不论是服务器部署、网络架构设计，都做到精细入微。因此，传统上的数据中心网络架构由于多层结构、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，导致网络结构比较复杂，使得数据中心基础网络的运维管理难度较高。 使用智能弹性架构(intelligent resilient framework, IRF)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 ”，并将这些设备看作单一设备进行管理和使用。多个盒式设备整合类似于一台机架式设备，多台框式设备的整合相当于

增加了槽位，虚拟化整合后的设备组成了一个逻辑单元，在网络中表现为一个网元节点，管理简单化、配置简单化、可跨设备链路聚合，极大简化网络架构，同时进一步增强冗余可靠性。