DPtech OVC 技术白皮书

杭州迪普科技有限公司

2013 年 9 月

目录

1 概述

随着网络规模日益扩大，组网日益复杂，传统的网络部署模型已难以满足日益多样化的需求和严格的安全要求。由于传统的组网部署方式存在组网复杂、维护成本高、多个部门间业务隔离手段单一、缺乏灵活的安全定制能力等诸多问题，用户强烈希望有一种技术，在不增加建设成本的情况下，实现网络中多业务和多部门间快速、灵活、可靠的 L2-7 层业务隔离和安全防护。

目前常见的解决方案通常使用 VRF 或 MPLS/VPN 进行域间隔离。这种部署方式存在两个缺点：其一，VRF 实例或 MPLS 标签进行软件隔离只是转发层面的隔离，无法在控制层面和管理层面做到隔离；其二，系统资源是共享和抢占式的，各隔离域没有固定的资源，无法实现资源预留和按需分配，也无法根据客户需求灵活定制隔离域的各项服务。

OVC（OS-Level Virtual Context，操作系统级虚拟环境）技术是一种将一台物理设备虚拟成多台逻辑设备的虚拟化技术。经过 OVC 虚拟化之后，同一台物理设备上的多个逻辑设备都拥有独立的硬件、软件、转发表项、管理平面和日志，各逻辑设备的运行互不影响。OVC 技术实现了资源和管理的虚拟化，物理设备资源池化后，业务的快速部署和调整不再受限于物理设备本身，实现了节约建设和运维成本、灵活按需部署、完全故障隔离等优点，有效地解决了多业务安全隔离和资源按需分配的问题。为网络和安全向动态的、弹性的云服务模式转变创造了基础条件。

2 OVC 技术介绍

2.1 基本技术术语定义

公共 OVC：系统初始状态存在的默认 OVC 实例，称为公共 OVC，所有资源归公共 OVC 统一使用。

普通 OVC：公共 OVC 外的其它 OVC 实例称为普通 OVC。创建普通 OVC 后，系统内任何没有划到普通 OVC 的资源都属于公共 OVC。

2.2 OVC 的架构与实现原理

OVC 技术是操作系统级别的虚拟化技术，能够实现 1:N 的虚拟化。OVC 系统架构如图 2-1 所示：

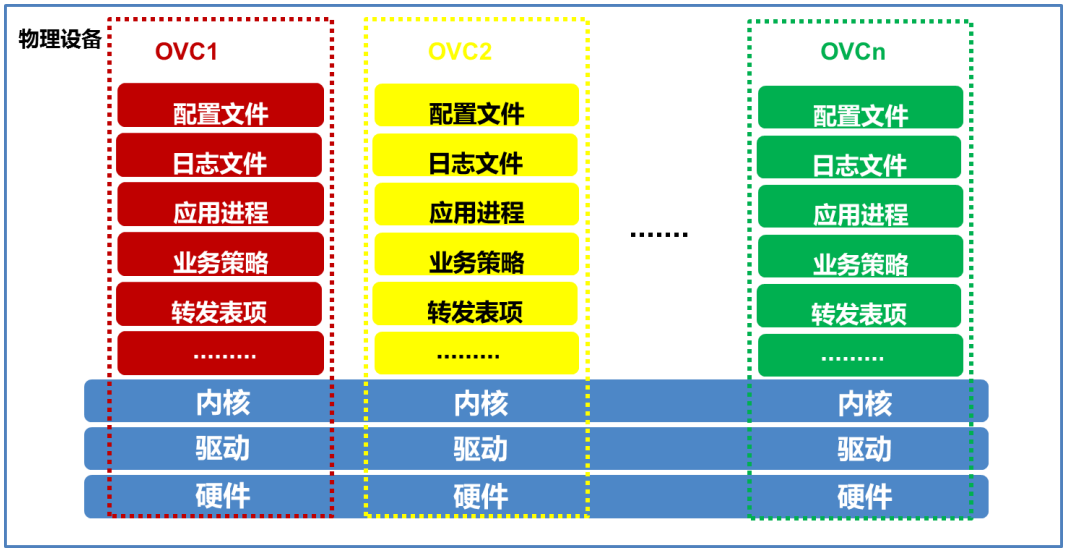


图 2-1 OVC 系统架构

通过操作系统级虚拟化技术，可以为每个 OVC 分配独立的端口、CPU、内存资源、会话数、新建、并发、吞吐量、路由表项数量、安全策略数量等一系列的软、硬件资源，灵活定制 OVC 的实际规格。

OVC 虚拟化技术使系统可以针对每个虚拟设备进行独立的进程管理、内存管理、磁盘管理，各虚拟设备之间没有切换和调度带来的资源消耗和性能损耗，同时通过操作系统虚拟化的支撑，可以实现各个 OVC 从管理平面、控制平面、数据平面、业务平面全方位隔离，形成各个完全独立的逻辑设备。操作系统内核完成 OVC 虚拟设备间的调度，并按预先设定的资源模板为各 OVC 虚拟设备分配硬件资源。

2.2.1管理平面虚拟化

如图 2-2 所示，OVC 实现物理设备的 1:N 虚拟化后，每个 OVC 可以看成独立的设备，用户可通过属于各 OVC 的网络接口访问并管理本 OVC。每个 OVC 拥有独

立的 HTTP/CLI/SNMP/SYSLOG 等配置管理协议进程，配置文件单独存放，可以独立进行重启和配置恢复。每个 OVC 拥有独立的管理员和日志文件，系统日志和操作日志可以独立输出到日志监控服务器。每个 OVC 由相应管理员自主管理，各个 OVC 之间互不可见。

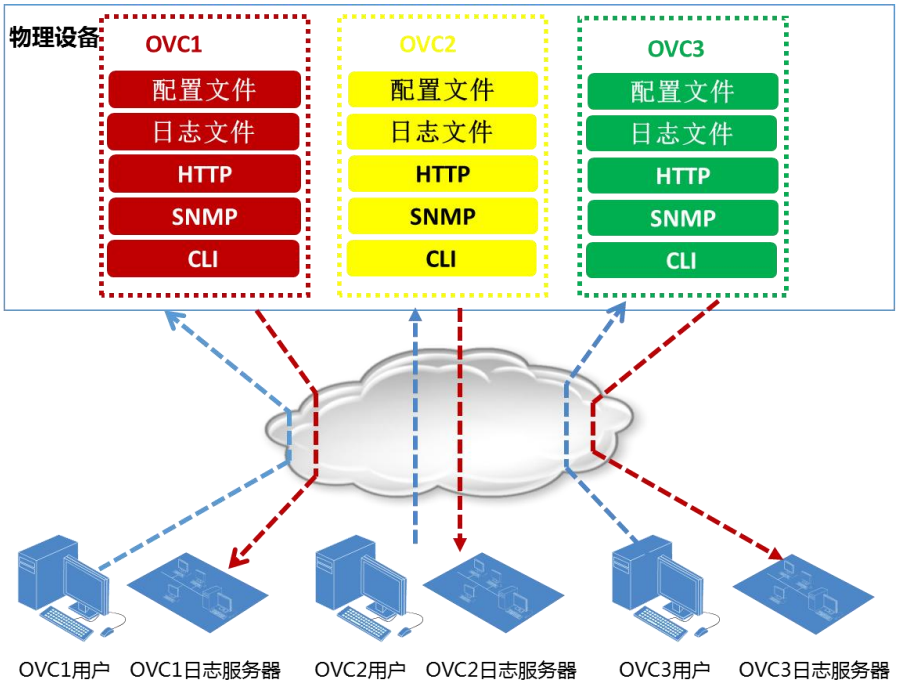


图 2-2 OVC 配置管理

2.2.2控制平面虚拟化

每个 OVC 会启动各自的管理进程对其所拥有的系统资源进行管理，也会启动各自的协议进程（如 OSPF、ISIS、BGP 等路由协议等）以维持各自的协议运行。每个 OVC 运行独立的协议进程，各进程间互不干扰。

如图 2-3 所示，OVC1 启用了 OSPF/ISIS，OVC2 启用了 OSPF/RIP/BGP，OVC3 启用了 ISIS/BGP，他们分别拥有独立的进程，任何 OVC 的协议进程故障不会影响其他 OVC 对应协议进程的正常运行。

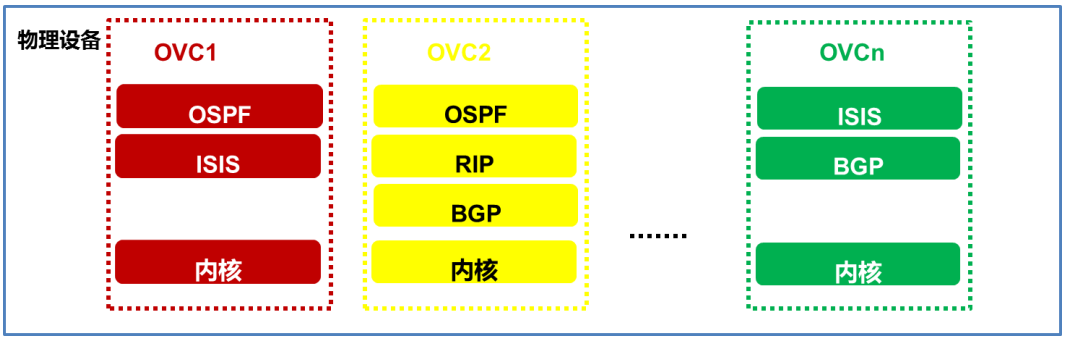


图 2-3 控制平面虚拟化

控制平面虚拟化带来的好处是 OVC 间的故障隔离。如图 2-4 所示，OVC2 内的 OSPF 进程崩溃导致该 OVC 的 OSPF 协议无法正常运行，而其它 OVC 内的 OSPF 进程仍然可以正常运行，完全不受其影响。

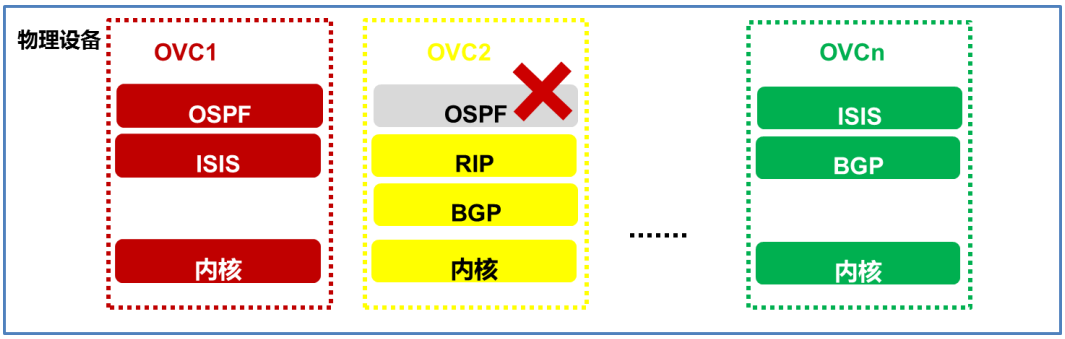


图 2-4 OVC 间的故障隔离

2.2.3数据平面虚拟化

当创建 OVC 时系统为之划分接口资源，这些接口由各自的虚拟数据平面管理，不同的 OVC 之间完全隔离。当流量从属于某一 OVC 的接口进入系统时，只会查询属于本 OVC 的转发表项，也只能从属于该 OVC 的接口转发出去，同时各种路由协议只能在这些接口资源上运行，确保每个 OVC 的转发表项只包含属于本 OVC 的接口，从而使不同 OVC 的路由和转发得到完全的隔离。

在安全设备上，报文转发时还需要建立会话表项，用于记录一些状态信息，为了保证每个 OVC 转发信息的完全隔离，每个 OVC 拥有独立的会话表，报文转发时只会查询、维护属于本 OVC 的会话表，各个 OVC 会话互不干扰，确保各个 OVC 的地址空间和转发信息完全独立。

2.2.4业务平面虚拟化

除了网络资源虚拟化外， OVC 虚拟化技术还实现了防火墙、IPS、负载均衡、流控、流量清洗等全系列 L4~7 层业务的虚拟化，将设备的网络、安全、应用交付资源全部池化，分解为不同粒度的服务资源，最高管理员在创建普通 OVC 并分配资源时可以灵活分配 L2~7 层全系列业务资源。

如图 2-5 所示，系统资源实现池化后，每个 OVC 可以独立配置相关业务的安全策略，独立处理自己的 L4~7 业务，不同 OVC 的安全业务完全隔离。彻底实现 L4~7 层的虚拟化。

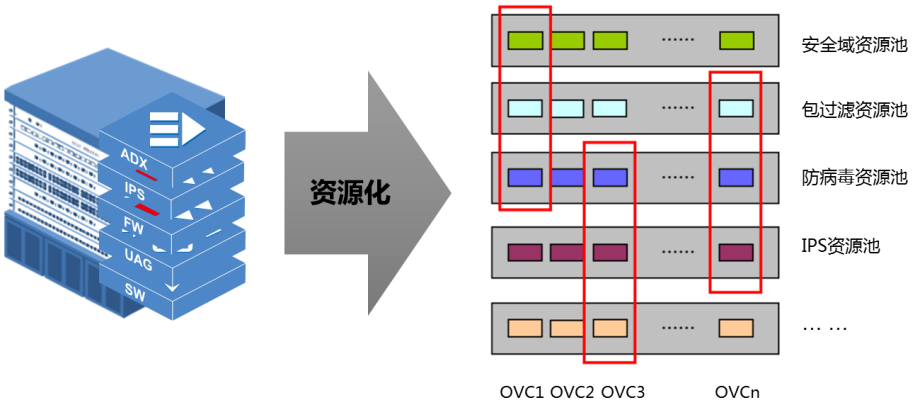


图 2-5 业务平面虚拟化

3 OVC 配置管理

设备支持 OVC 功能后，整台物理设备就是一个默认的 OVC，即公共 OVC，其拥有对整台物理设备的所有配置管理权限，可以管理设备所有的硬件资源，可创建、删除普通 OVC 并为其分配各类软、硬件资源。下面对 OVC 的创建删除、管理员分配、资源分配等配置管理操作逐一说明。

3.1 OVC 创建和删除

创建 OVC 时，需要指定 OVC 所属的虚拟管理系统。公共 OVC 不属于任何虚拟管理系统。普通 OVC 可以指定是否开启管理服务，开启的情况下系统会为该 OVC 独立创建 WEB 服务进程，以支持其通过 WEB 界面登录管理。如图 3-1 所示。

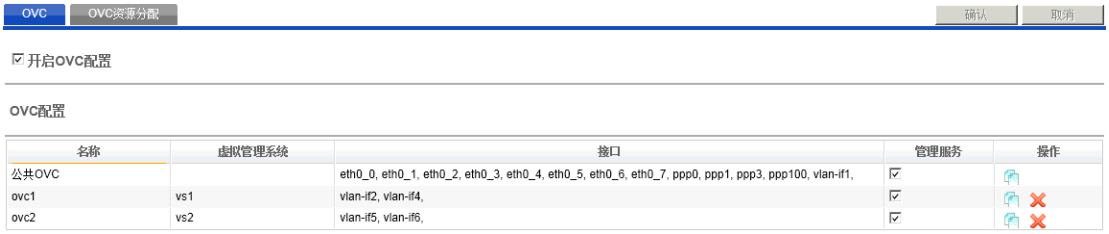


图 3-1 OVC 创建或删除配置界面

公共 OVC 不可被删除。删除普通 OVC 时，其所拥有的资源全都回归公共 OVC。

3.2 OVC 管理员配置管理

OVC 的管理员可以分为如下三个级别：

（1）**系统最高权限管理员：**该管理员只存在于公共 OVC，能够管理操作系统所有功能、查看所有配置和运行状态。只有本级管理员有权限开启或关闭 OVC 功能、创建或删除 OVC、为各 OVC 划分软、硬件资源及创建删除管理员等操作。整机重启、更换设备运行版本等全局操作也只能由本级别管理员进行。

（2）**普通 OVC 系统管理员：**该管理员是除公共 OVC 以外各普通 OVC 的系统管理员。系统最高权限管理员应在创建普通 OVC 的同时为其创建本级别管理员，否则该 OVC 无法通过其它途径进行配置管理。本级别管理员能够在由系统最高权限管理员为本 OVC 指定的权限范围内操作本 OVC 的系统资源、管理本 OVC 的功能模块，包括为本 OVC 的接口配置 IP 或其它属性、基于本 OVC 的接口配置安全策略、配置本 OVC 系统日志监控设备的地址等。

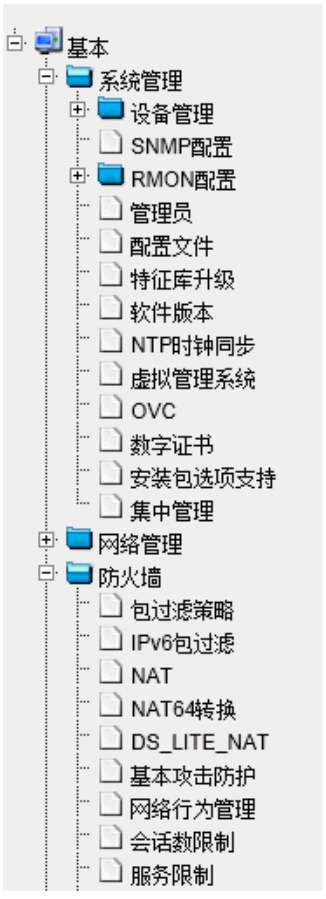
（3）**普通 OVC 管理员：**该级别管理员可以存在于所有普通 OVC 中，其只能在前两级管理员为其指定的配置权限内进行配置管理，其配置管理范围是本 OVC 的系统管理员的配置管理范围的一个子集。

普通 OVC 的系统管理员只能查看并管理自己所属 OVC 的管理员以及该 OVC 内其它配置，各 OVC 配置相互不可见。

如图 3-2 所示，系统中存在 4 名管理员，分别为 admin（系统最高权限管理员）、ovc1_admin（虚拟管理系统 vs1 的系统管理员）、ovc2_admin（虚拟管理系统 vs2 的系统管理员）、ovc2_user（虚拟管理系统 vs2 的普通用户，仅有日志查看等权限）。

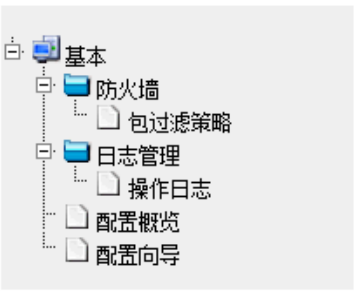
图 3-2 OVC 管理员配置

如图 3-3 所示，不同级别的管理员所能配置管理的功能各不相同。



admin登录界面菜单

ovc2_admin登录界面菜单



ovc2_user登录界面菜单

图 3-3 各级管理员登录界面菜单

普通 OVC 系统管理员只能查看并配置本 OVC 的资源。

如图 3-4 所示，由于系统最高权限管理员 admin 只为 ovc1 分配了 vlan-if2 和 vlan-if4 两个接口，所以 ovc1_admin 访问源 NAT 配置页面时，只能从 ovc1 所拥有的这两个接口中选择出接口。

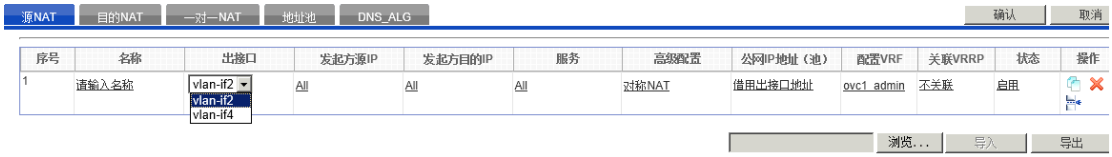


图 3-4 ovc1 管理员 ovc1_admin 访问源 NAT 配置页面

类似地，ovc2 的管理员登录后也只能从自己所拥有的接口列表 vlan-if5、vlan-if6 中选择接口。如图 3-5 所示：

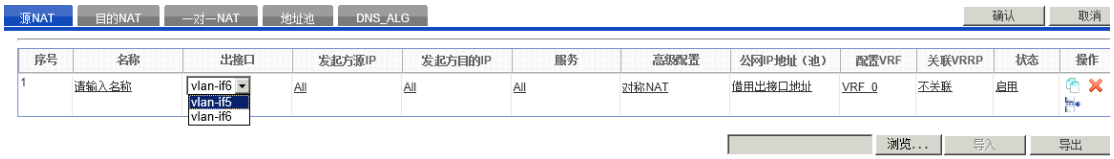


图 3-5 ovc2 管理员 ovc2_admin 访问源 NAT 配置页面

3.3 OVC 资源分配管理

OVC 可供分配的资源包括物理或逻辑接口、CPU、内存、磁盘、会话数、新建会话速率、吞吐量等。

如图 3-6 所示，公共 OVC 系统管理员 admin 访问 OVC 资源分配页面时，可为各 OVC 分配资源。普通 OVC 的管理员访问该页面时，只能查看和配置本 OVC 的资源。

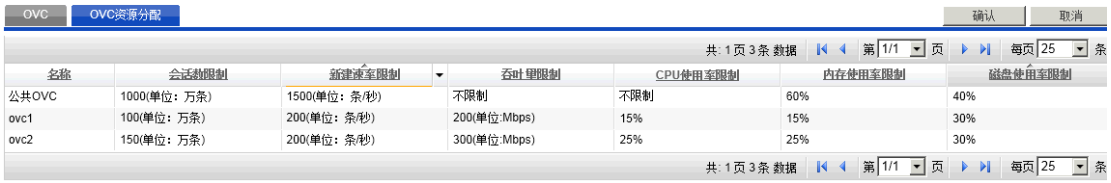


图 3-6 admin 访问 OVC 资源分配页面

4 VSM 与 OVC 结合虚拟化

4.1 VSM 虚拟化技术简介

VSM（Virtual Switching Matrix），虚拟交换矩阵，是将多台物理设备虚拟化成一台逻辑设备的技术。设备间的协同工作不再需要用户关注，从而使组网和管理得到简化、性能和效率得到提升。同时，通过 VSM 的在线扩容和在线升级技术，部署了 VSM 技术的网络环境可以在不改变原有网络拓扑的情况下向现有网络增加 VSM 成员设备，使整个逻辑设备拥有更多硬件和软件资源、更强大的处理能力。

4.2 VSM 与 OVC 结合的虚拟化

VSM 将多台物理设备虚拟化成一台逻辑设备，而 OVC 将一台设备虚拟化成操作系统级别的多台逻辑设备。将 VSM 虚拟成的逻辑设备进行 OVC 虚拟化，则可以实现 N:M 的虚拟化，即在 N 台物理设备上运行 M 个 OVC 系统，N 与 M 之间不存在比例限制。

将 VSM 和 OVC 结合的虚拟化技术，可以在提供 OVC 虚拟化节约建设成本、快速部署等优点的基础上大大提高系统可靠性。

迪普科技目前可以提供 L2~7 层全业务的 N:M 虚拟化。如图 4-2 所示，将两台部署了 IPS、防火墙、负载均衡板卡的物理设备通过 VSM 技术形成一台逻辑设备，同时采用 OVC 技术拆分成多台具备虚拟 IPS、虚拟防火墙、虚拟负载均衡的虚拟设备，每台虚拟设备可以提供完全独立的 L2~7 层业务。

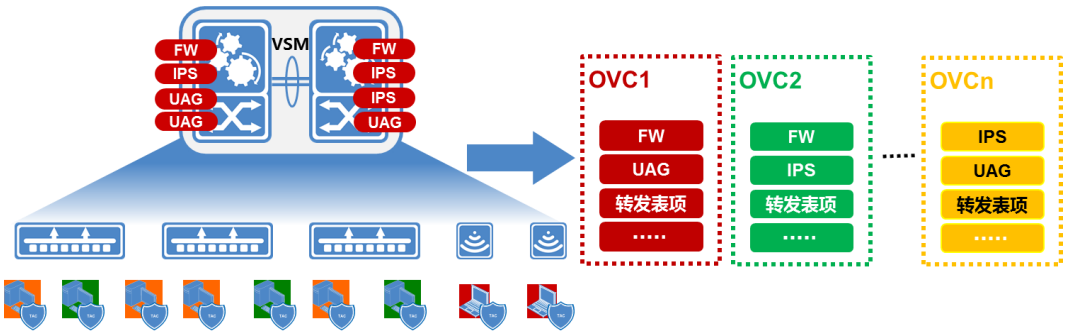


图 4-2 N:M 业务虚拟化

5　典型组网应用举例

OVC 技术既可独立应用在实际组网中，也可与 VSM 技术结合使用。具体如何使用取决于实际环境的规模、组网模式、带宽要求、可靠性要求等方面。下面就两种典型的组网环境示例说明。

5.1 常见组网 1：业务部门隔离

在园区网中，可能存在内网和外网两个用户群，内网用户只允许访问内网服务器，外网用户只允许访问外网服务器。传统的组网方式中，必须对内网和外网分别组建一个物理网络，对两个网络的流量进行物理隔离，这样必将耗费大量硬件成本、运营成本和管理成本。

采用 OVC 技术后，内网和外网只需组建一套物理网络，在相关设备上将内网、外网用户/服务器所连接口分别划分到不同的 OVC 中，并在各自 OVC 中创建管理员账户进行管理维护即可，极大地节省硬件成本和维护成本。组网如图 5-1 所示：

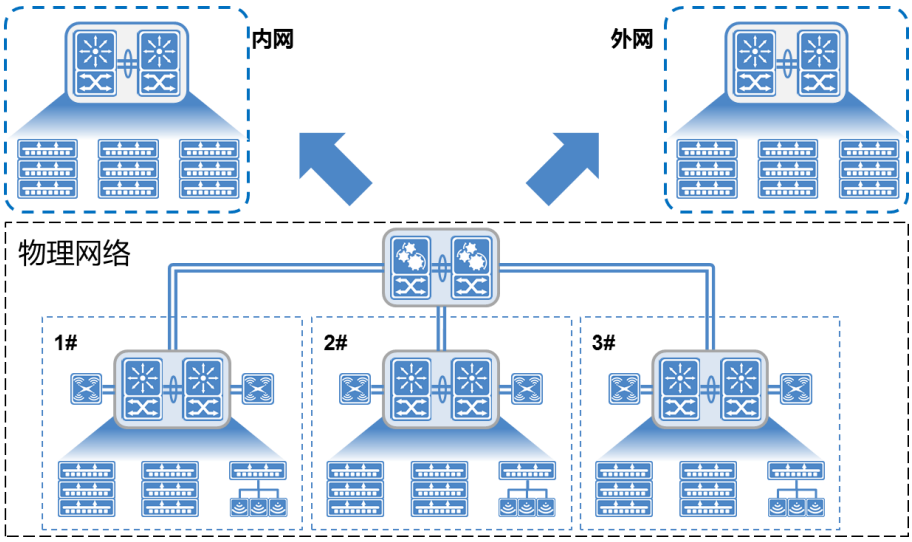


图 5-1 业务部门隔离组网

5.2 常见组网 2：多租户 IaaS 应用

在当前云计算时代，IaaS 已经成为越来越流行的 IT 建设模式，企业用户向运营商或云服务提供商购买或租用网络和安全设备。运营商或云服务提供商如何

以更经济的、灵活的方式为大量企业用户提供网络和安全服务是一个挑战，OVC 技术可以解决这个问题。

如图 5-2 所示，采用 OVC 技术后，实际上用户购买或租用的不是物理设备，而是通过 OVC 技术创建的虚拟设备。通过 OVC 虚拟化技术从物理设备上划分的一部分资源组成虚拟设备给用户使用，不必为每个用户单独购买组建网络的全套设备，用户可以通过运营商提供的管理员账户，对自己租用或购买的虚拟设备按需进行灵活配置管理。当企业网络规模需要调整时，也可以随时向运营商申请增加或减少本虚拟设备的软硬件接口等资源，既不需要调整组网，也不需要另行购买和安装设备。

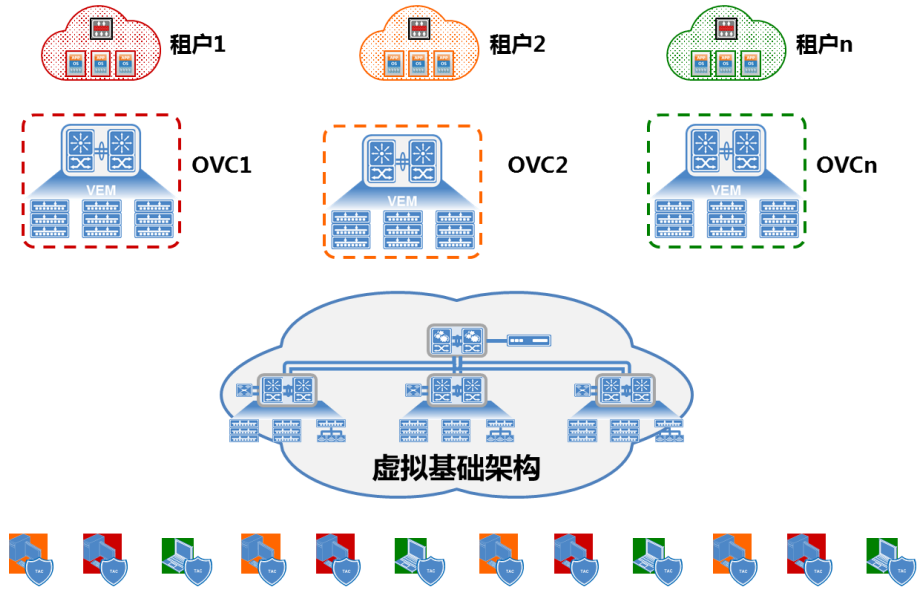


图 5-2 多租户 IaaS 应用