VMware® NSX
网络虚拟化
设计指南

目录

目标读者

本文档面向想要部署 VMware® 网络虚拟化解决方案的虚拟化和网络架构师。

概述

IT 组织已经直接从服务器虚拟化中获得了显著好处。服务器整合降低了物理复杂性，提高了运营效率，并且能够动态地重新调整底层资源的用途，以便以最佳方式快速满足日益动态化的业务应用需求，而这些只是已经实现的众多好处中的少数几个。

现在，VMware 的软件定义的数据中心（SDDC）体系结构正在跨整个物理数据中心基础架构扩展虚拟化技术。VMware NSX 网络虚拟化平台是 SDDC 体系结构中的一款重要产品。使用 NSX，现在可以对网络提供已对计算和存储实现的相同虚拟化功能。就像服务器虚拟化可以通过编程方式创建、删除和还原基于软件的虚拟机（VM）以及拍摄其快照一样，NSX 网络虚拟化也对基于软件的虚拟网络实现这些同样的功能。结果是一种具有彻底革命性的联网方法，不仅使数据中心管理人员能够将敏捷性和经济性提高多个数量级，而且还能大大简化底层物理网络的运营模式。NSX 能够部署在任何 IP 网络上，包括现有的传统网络模型以及任何供应商提供的新一代体系结构，是一个完全无中断的解决方案。事实上，使用 NSX，您已经拥有的物理网络基础架构就是部署软件定义的数据中心所需的全部基础。

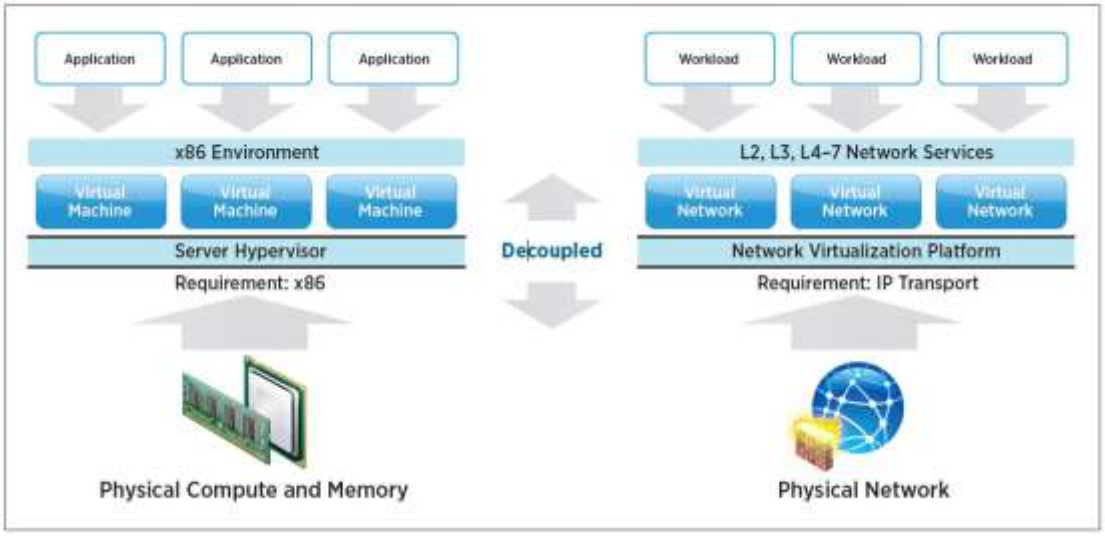

图 1. 服务器和网络虚拟化类比

图 1 对计算和网络虚拟化进行了类比。实现服务器虚拟化后，软件抽象层（服务器虚拟化管理程序）可在软件中重现人们所熟悉的 x86 物理服务器属性（例如 CPU、RAM、磁盘、网卡），从而可通过编程方式以任意组合来组装这些属性，只需短短数秒，即可生成一台独一无二的虚拟机（VM）。

实现网络虚拟化后，与“网络虚拟化管理程序”等效的功能可在软件中重现第 2 层到第 7 层的一整套网络服务（例如，交换、路由、访问控制、防火墙、QoS 和负载平衡）。因此，可通过编程方式以任意组合来组合这些服务，只需短短数秒，即可生成独一无二的隔离式虚拟网络。

当然，也可以提供类似的优势。例如，就像虚拟机独立于底层 x86 平台并允许 IT 将物理主机视为计算容量池一样，虚拟网络也独立于底层 IP 网络硬件并允许 IT 将物理网络视为可以按需使用和调整用途的传输容量池。与旧式体系结构不同，可以编程方式调配、更改、存储、删除和还原虚拟网络，而无需重新配置底层物理硬件或拓扑。这种革命性的联网方法能够与企业从熟悉的服务器和存储虚拟化解决方案获得的能力和优势相匹配，从而可发挥软件定义的数据中心的全部潜能。

有了 VMware NSX，您就有了部署新一代软件定义的数据中心所需的网络。本文将重点介绍为了充分利用您的现有网络投资并通过 VMware NSX 优化该投资，您应该考虑的设计因素。

VMware NSX 解决方案的组件

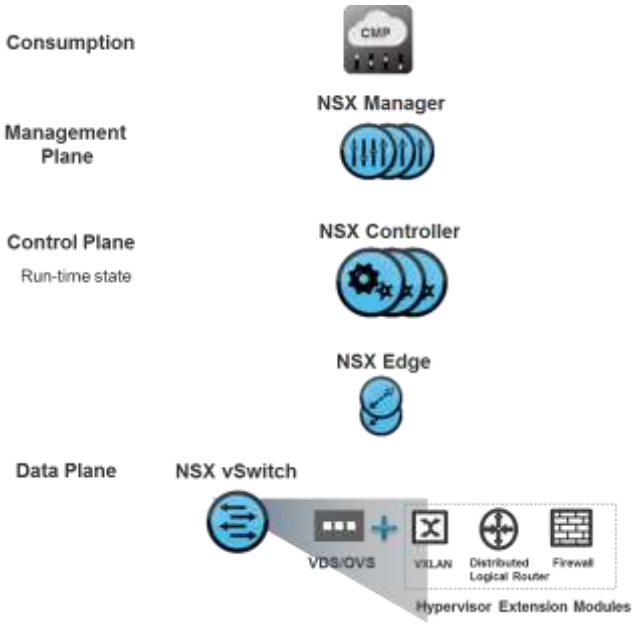

图 2.VMware 网络虚拟化解决方案组件

数据板

NSX 数据板由 NSX vSwitch 组成。NSX for vSphere 中的 vSwitch 基于 vSphere Distributed Switch (VDS)（或用于非 ESXi 虚拟化管理程序的 Open vSwitch），还包括其他组件，可提供丰富的服务。附加 NSX 组件包括在虚拟化管理程序内核中运行的用于提供分布式路由、分布式防火墙等服务并实现 VXLAN 桥接功能的内核模块 (VIB)。

NSX vSwitch（基于 VDS 或 OVS）可对物理网络进行抽象化处理并在虚拟化管理程序中提供访问级别的交换。它对网络虚拟化至关重要，因为它可实现独立于物理构造的逻辑网络（例如 VLAN）。vSwitch 的一些优势包括：

- 利用 VXLAN、STT、GRE 等协议以及集中式网络配置支持覆盖网络。覆盖网络可实现以下功能：
  - 在现有物理基础架构上创建一个覆盖现有 IP 网络的灵活的逻辑层 2（第 2 层），而无需重新设计任何数据中心网络
  - 配置通信（东西向和南北向），同时让租户之间保持相互隔离
  - 应用工作负载和虚拟机独立于覆盖网络，并且就像连接到物理第 2 层网络一样运行
- NSX vSwitch 有利于实现虚拟化管理程序的大规模扩展。
- 端口镜像、NetFlow/IPFIX、配置备份和还原、网络运行状况检查、QoS 和 LACP 等多种功能可在虚拟网络内提供一个全面的流量管理、监控和故障排除工具包。

此外，数据板还包含网关设备，这些设备可提供从逻辑网络空间 (VXLAN) 到物理网络 (VLAN) 的第 2 层桥接。网关设备通常是NSX Edge 虚拟设备。NSX Edge 提供第 2 层、第 3 层、外围防火墙、负载平衡和 SSL VPN、DHCP 等其

他服务。

从虚拟网络到物理网络的第 2 层桥接功能也可以由支持解封 VXLAN 流量的功能的物理网络交换机实现。

控制板

NSX 控制板在 NSX Controller 中运行。在采用 VDS 的 vSphere 优化环境中，控制器可实现自由多播 VXLAN 以及 VDR 等元素的控制板编程。在多虚拟化管理程序环境中，控制器节点对 vSwitch 转发板进行编程。

无论是哪种情况，控制器都只是控制板的一部分，不会有任何数据板流量通过它传递。控制器节点还部署在具有奇数个成员的集群中，以实现高可用性和可扩展性。控制器节点发生任何故障都不会对数据板流量造成任何影响。

管理板

NSX 管理板由 NSX Manager 构建。NSX Manager 在 vSphere 环境中为 NSX 提供单个配置点和 REST API 入口点。

使用平台

可以直接通过 NSX Manager UI 使用 NSX。在 vSphere 环境中，可通过 vSphere Web UI 本身使用。通常，在网络虚拟化中，终端用户与其云管理平台联系在一起，以部署应用。NSX 通过 REST API 提供一组丰富的集成功能，几乎可集成到任何 CMP。还可通过 VMware vCloud Automation Center、vCloud Director 以及具有用于 NSX 的 Neutron 插件的 OpenStack，获得开箱即用的集成功能。

NSX for vSphere 的功能服务

在本设计指南中，我们将讨论上面描述的所有组件如何为我们提供以下功能服务：

- **第 2 逻辑层** – 在结构中的任何位置实现第 2 层网段/IP 子网的扩展，而无需考虑物理网络设计
- **第 3 层分布式路由** – IP 子网之间的路由可以在逻辑空间中完成，不会有流量传出到物理路由器。这种路由是在虚拟化管理程序内核中执行的，CPU/内存开销极少。这种功能可为虚拟基础架构内的流量路由提供最佳数据路径。同样，NSX Edge 提供一种使用 OSPF、BGP 和 IS-IS 与物理网络进行全面的动态路由配对的机制，以实现无缝集成。
- **分布式防火墙** – 安全保护措施在内核以及虚拟网卡级别本身执行。这将能够以高度可扩展的方式实施防火墙规则，而不会在物理设备上造成瓶颈。防火墙分布在内核中，因此只产生极少的 CPU 开销，并且能够以线速执行。
- **逻辑负载平衡** – 支持第 4 层到第 7 层负载平衡，并且能够执行 SSL 端接。
- SSL VPN 服务，可实现第 2 层 VPN 服务。

网络虚拟化设计注意事项

VMware 网络虚拟化可以在现有数据中心网络上部署。在本节中，我们将讨论如何在常见的数据中心网络拓扑中部署使用 VXLAN 的逻辑网络。首先，我们介绍对物理网络的要求，然后探讨最适合网络虚拟化的网络设计。最后，我们介绍逻辑网络和相关服务以及扩展注意事项。

物理网络

在不同的用户环境中，物理数据中心网络在数据中心中使用的网络拓扑不同。分层网络设计可提供数据中心网络所需的高可用性和可扩展性。本节假定读者了解利用传统第 3 层和第 2 层网络配置的各种网络拓扑的背景知识。建议读者查看其所选物理网络供应商的设计指南。在下面几节中，我们将介绍最常见的物理网络拓扑，并分析如何在这些情景中实现网络虚拟化。

数据中心结构属性

网络虚拟化的重要目标之一是提供虚拟网络到物理网络的抽象化处理。物理结构必须提供具有以下特点的可靠 IP 传输：

- 简单
- 可扩展
- 高带宽
- 容错
- 提供 QoS

下面几节分别提供这些特点的详细信息。在下面的讨论中，“访问层交换机”、“架顶式（ToR）交换机”和“分支交换机”这几个术语可以互换。分支交换机通常位于机架内，为该机架内的服务器提供网络访问。“聚合层”和“主干层”（用于有效提供机架之间的连接）这两个术语是指网络中聚合所有访问交换机的位置。

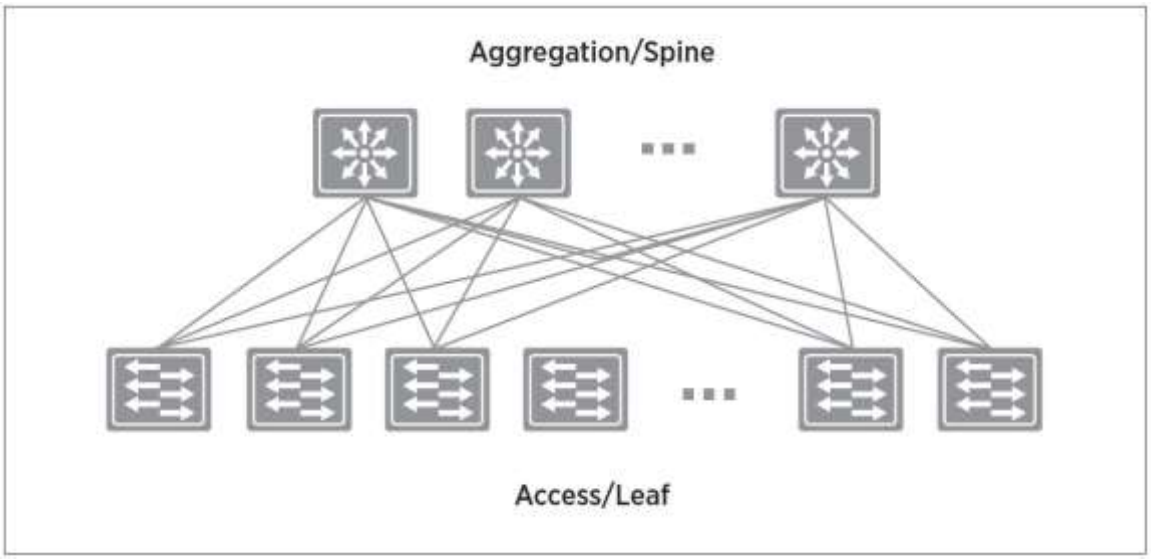

图 3. 分支-主干拓扑

简单

组成数据中心内的整体结构的交换机的配置必须简单。无论交换机位于何处，诸如 AAA、SNMP、SYSLOG、NTP 等常规或全局配置都应该逐行复制。下面是数据中心结构设计连接方式的主要示例：

分支交换机

面向机架内的服务器的端口应具有最低配置。图 4 是分支节点的简要的物理和逻辑表示图。

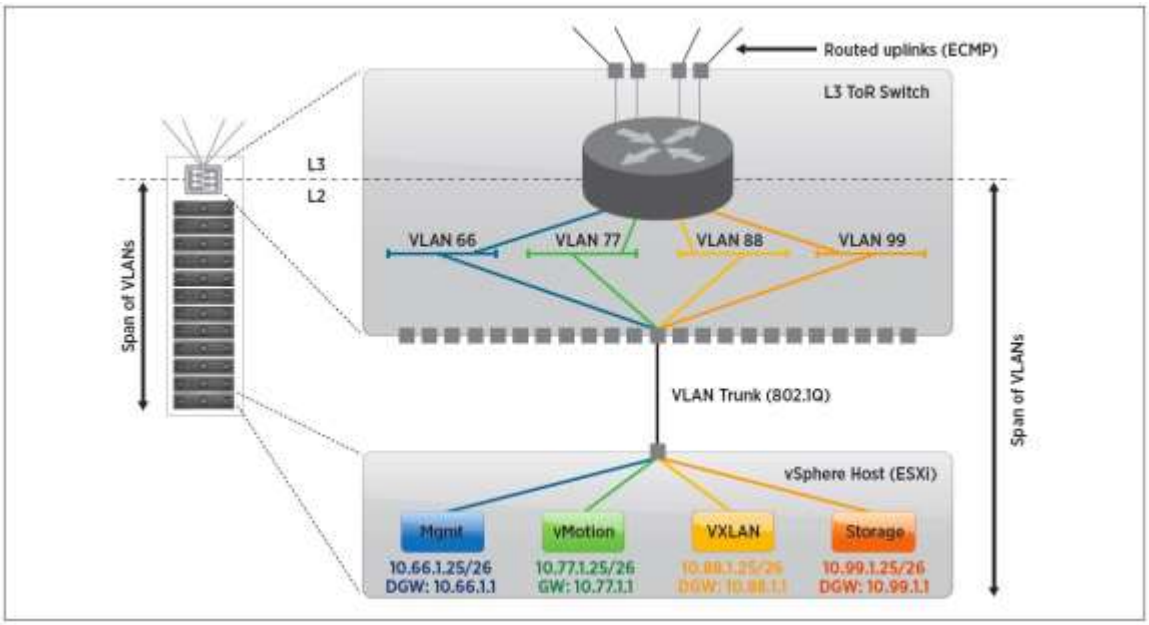

图 4. 分支节点的简要的物理和逻辑表示图

假定服务器具有多个相同速度的接口，则可以使用链路聚合。vSphere Distributed Switch 上提供了多种链路聚合选项。其中两个重要选项是基于负载的绑定（其路由基于虚拟网络适配器负载）以及基于 IEEE 802.3ad 标准的链路聚合控制协议 (LACP)。使用绑定选项可最好地利用可用带宽，同时还可提供可应对应对链路故障的高可靠性。

通常，801.Q 主干用于支持少量 VLAN；例如 VXLAN 安全加密链路、管理存储和 VMware vSphere vMotion® 流量。交换机分别针对每个 VLAN 终止和提供默认网关功能；即，它为每个 VLAN 提供一个交换机虚拟接口 (SVI)。从 ToR 交换机或分支交换机到聚合或主干层的上行链路是点对点路由链路。不允许在上行链路中使用 VLAN 中继，甚至对于单个 VLAN 也不行。将在分支和主干交换机之间配置动态路由协议（例如 OSPF、ISIS、BGP）。机架中的每个 ToR 交换机都会通报几个前缀，通常是一个 VLAN 或一个子网一个前缀。进而，它将根据从其他 ToR 交换机收到的前缀计算等成本路径。在 vSphere 环境中，vSphere vMotion 和存储网络有一些设计限制。“数据中心访问层中的第 3 层”一节中将详细讨论这些限制。

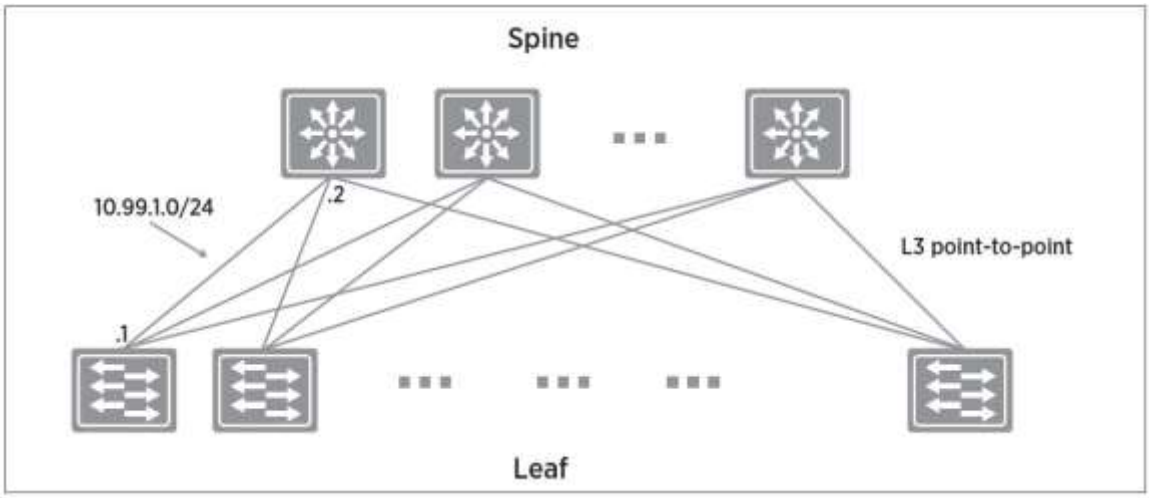

图 5. 分支和主干交换机之间的第 3 层连接

主干交换机

主干交换机只有连接到分支交换机的接口；所有接口均配置为点对点路由链路，能有效充当分支交换机的点对点上行链路的“另一端”。

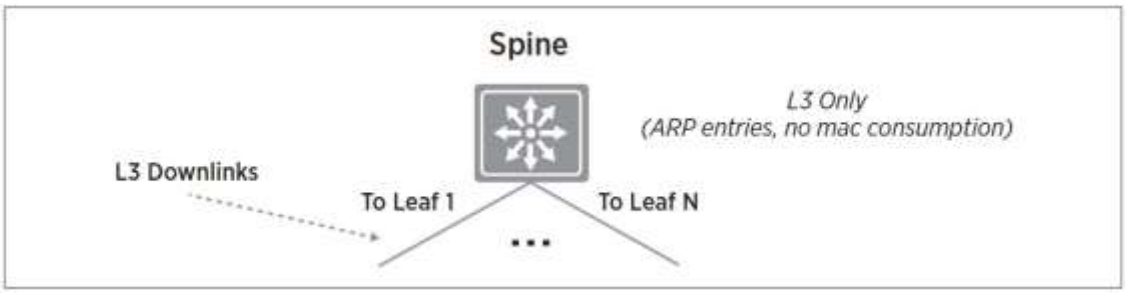

图 6. 主干交换机接口

主干交换机之间通常不需要链路。如果主干交换机和分支交换机之间的链路出现故障，路由协议将确保不会将受影响机架的流量引到已与该机架断开连接的主干交换机。

可扩展

与扩展能力有关的因素包括结构中支持的机架数量、数据中心中任何两个机架之间存在的带宽、分支交换机在与另一机架通信时可以选择的路径数量，等等。

结构中支持的机架数量由所有主干交换机中的可用端口总数以及可接受的超额预订比率确定。更多详细信息，请参见“高带宽”一节。

不同的机架可能托管不同类型的基础架构。例如，可能存在包含文件服务器或其他存储系统的机架。从其性质上看，此类机架可能会比数据中心中的其他机架吸引或输出更多流量。此外，与用于连接到外部环境的边缘机架不同，计算机架（即，托管包含工作负载或虚拟机的虚拟化管理程序的机架）的流量级别可能具有不同的带宽要求。为了满足不同的带宽要求，链路速度以及链路数量会有所不同。可以针对每个机架做出调整，而不影响主干交换机或分支交换机的任何体系结构。

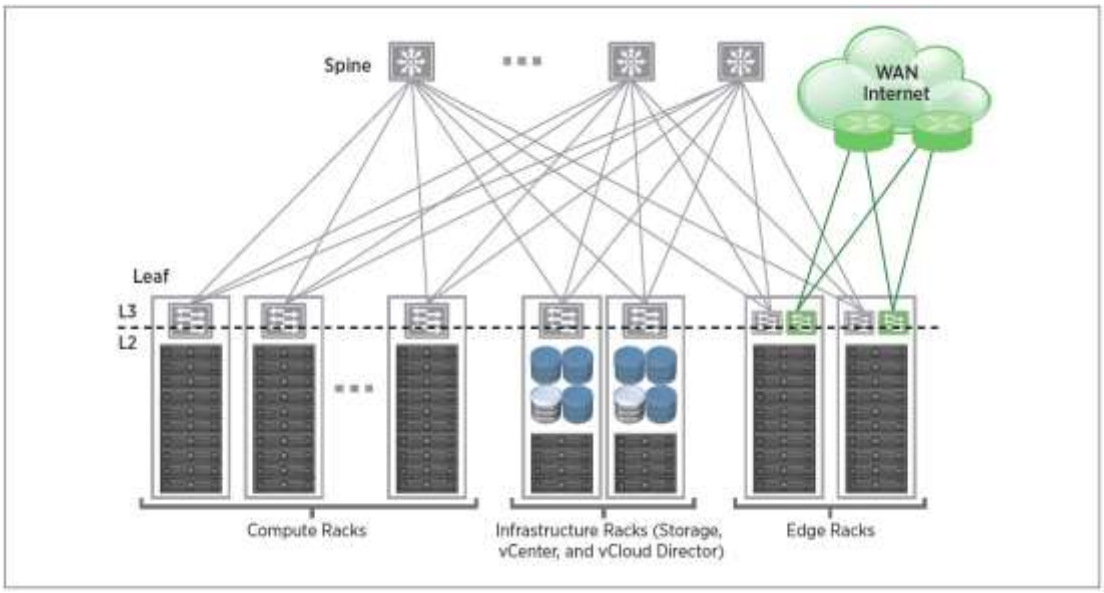

图 7. 分支-主干拓扑中的计算、基础架构和边缘机架设计

与主干交换机之间的链路的数量确定了从此机架到其他机架的流量可以选择的路径的数量。由于任何两个机架之间的跃点数是一致的，因此可以利用等成本多路径 (ECMP) 策略。假定服务器输出的流量带有 TCP 或 UDP 标头，则每个通信流都可能会发生四处传输流量的现象。

高带宽

在主干-分支交换机拓扑中，如果发生超额预订，则通常发生在一个位置，即分支交换机。计算方式非常简单：可供连接到给定分支交换机的所有服务器使用的总带宽量除以聚合的上行链路带宽量就是超额预订比率。例如，20 台各具有一个 10 Gb 以太网（10 GbE）端口的服务器可产生最多 200 Gbps 的带宽。假定有 8 个 10 GbE 上行链路链接到主干，即总共 80 Gbps，则超额预订比率是 2.5:1。

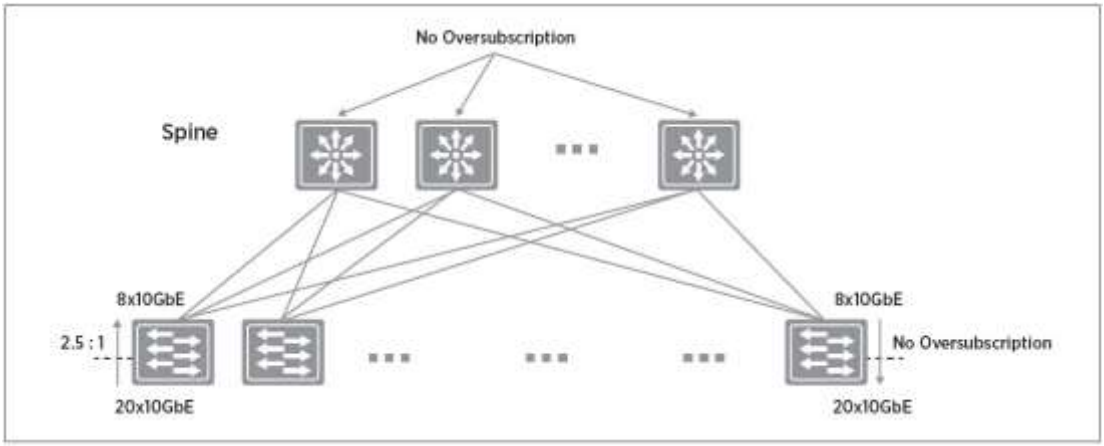

图 8. 分支-主干拓扑的超额预订示例

如上一节所述，根据机架的功能，可以通过调配更多或更少上行链路，向机架提供更多或更少带宽。换句话说，每个机架的超额预订级别可能不同。

从体系结构的角度看，必须遵循一条规则：从分支交换机到每个主干交换机的上行链路数量必须相同；即，到主干交换机 A 有两条上行链路，而到主干交换机 B、C 和 D 只有一条上行链路，这样的设计欠佳，因为将会有“更多”流量通过主干交换机 A 发送到分支交换机，从而可能产生热点。

容错

环境越大，构成整体结构的交换机就越多，数据中心交换结构的一个组件出现故障的可能性也越大。应构建具有恢复能力的结构的理由是，它可以承受单个链路或服务器故障，而不会产生大范围影响。

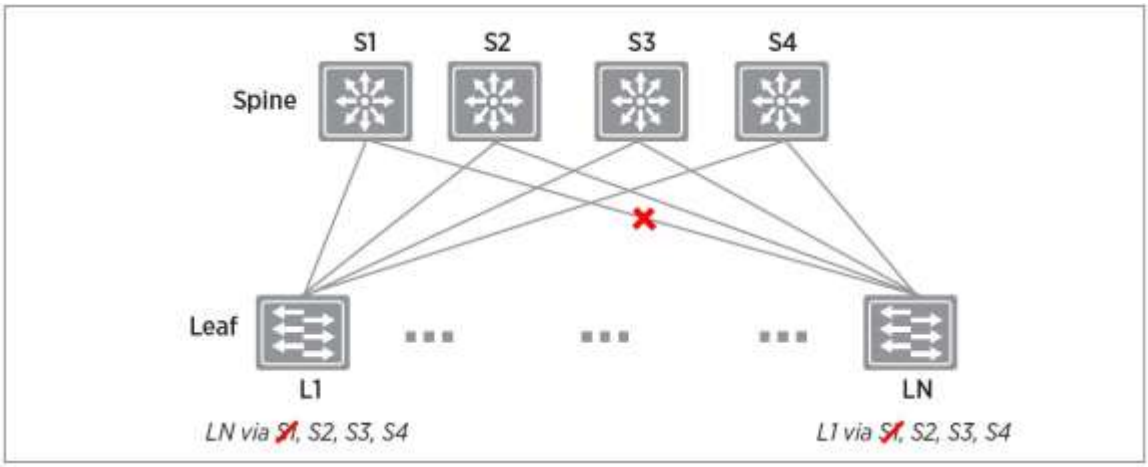

图 9. 分支-主干拓扑中的链路故障情景

例如，如果一个主干交换机出现故障，机架之间的流量将继续通过剩余的主干交换机在第 3 层结构中路由。对于第 3 层结构，路由协议可确保只能选择剩余的路径。此外，由于可以安装两个以上的主干交换机，因此可以减少主干交换机故障所产生的影响。

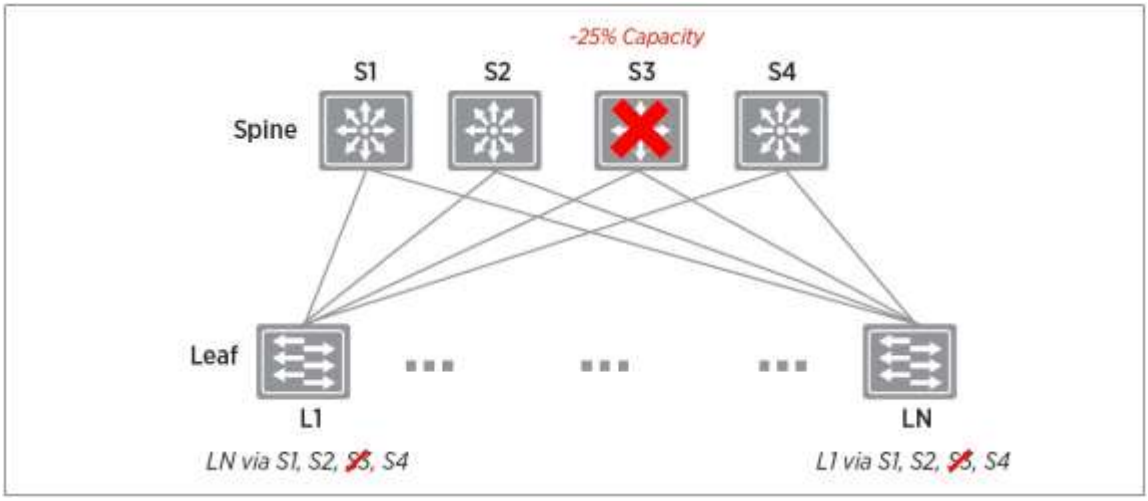

图 10. 主干交换机故障情景及其对带宽的影响

支持多路径的结构可处理服务器或链路故障，从而减少手动执行网络维护或操作的需要。如果必须对结构交换机进行软件升级，则可以通过更改路由协议指标使节点平稳地退出使用；通过该交换机的流量很快就会从该交换机抽离出来，从而释放交换机以便进行维护。根据主干的宽度（即，聚合或主干层中有多少台交换机），其余交换机必须承担的额外负载不像聚合层中只有两台交换机时那么多。

差异化服务 - 服务质量

虚拟化环境必须跨交换基础架构传送各种类型的流量，包括租户、存储和管理流量。每种流量都具有不同的特征，对物理交换基础架构也有不同的要求。虽然管理流量通常较少，但它对于控制物理和虚拟网络状态却至关重要。IP 存储流量通常较多，并且一般位于数据中心内。云运营商可能会为租户提供各种级别的服务。整个结构中不同租户的流量具有不同的服务质量（QoS）值。

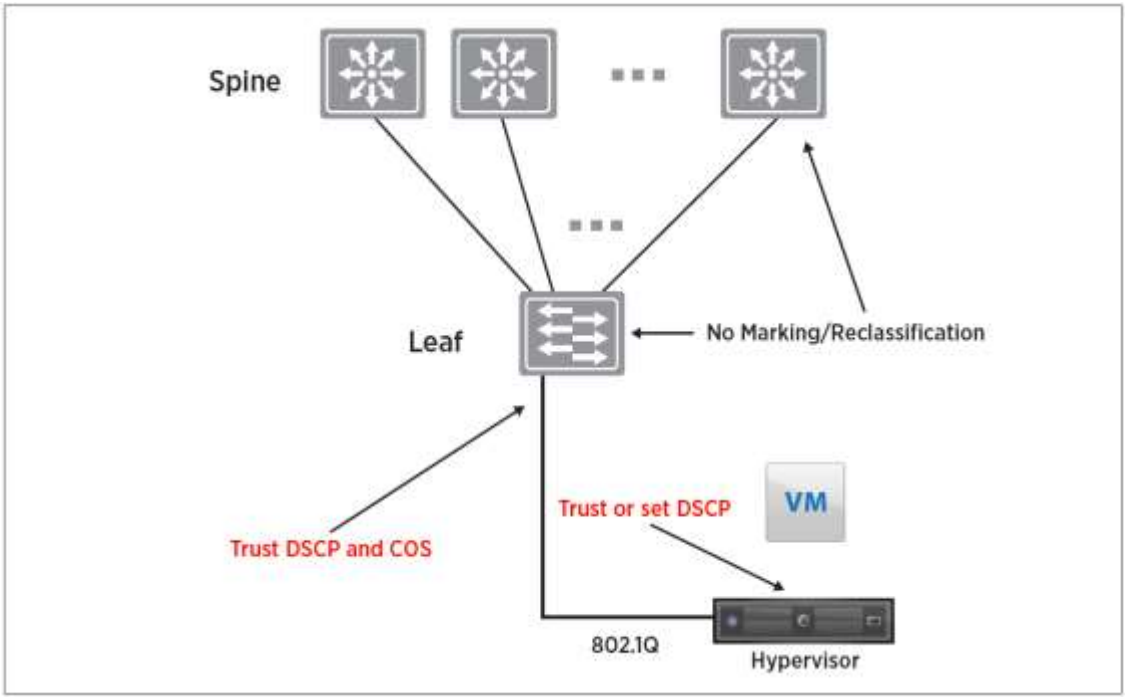

图 11. 服务质量（QoS）标记

对于虚拟化环境，虚拟化管理程序会显示可信边界，这意味着它会为不同的流量类型设置相应的 QoS 值。在这种情况下，物理交换基础架构应该“信任”这些值。不需要在面向服务器的分支交换机端口上重新分级。如果物理交换基础架构中存在拥塞点，将检查 QoS 值，以确定应如何设定流量的顺序或优先级，并且可能需要丢弃流量。

物理交换基础架构中支持两种类型的 QoS 配置；一种在第 2 层处理，另一种在第 3 层或 IP 层处理。第 2 层 QoS 有时称为“服务等级”，第 3 层 QoS 称为“DSCP 标记”。在 VMware vSphere 5.5 版中，服务等级和 DSCP 标记均受支持，用户可以基于流量类型或数据包分类方法标记流量。当虚拟机连接到基于 VXLAN 的逻辑交换机或网络时，来自内部数据包标头的 QoS 值将被复制到 VXLAN 封装的标头。这使外部物理网络能够基于外部标头中的标记设定流量的优先级。

数据中心访问层部署情景

本节讨论如何基于可扩展的网络结构实施网络虚拟化。网络虚拟化主要包含三个方面：分离、重现和自动化。要实现所需效率，这三个方面全都非常重要。本节重点介绍分离，它是简化和扩展物理基础架构的关键。网络虚拟化解决方案只能按照可扩展结构提供的方式使用连接选项，具体说就是，网络虚拟化解决方案不能使 VLAN 超出交换基础架构内单个机架的范围。

在本设计指南中，我们将考虑数据中心访问层中的第 3 层设计。

数据中心访问层中的第 3 层

在构建新环境时，选择允许未来增长的体系结构很有必要。此处讨论的方法适用于从小规模开始逐步扩展为大规模、同时在整体上仍然保留相同体系结构的部署。

此类部署的指导原则是，网络虚拟化解决方案并不意味着 VLAN 能超出单个机架的范围。尽管这似乎是一个很简单的要求，但它却对物理交换基础架构的构建方式和扩展方式具有广泛影响。

我们将分别介绍基础架构内的以下三种不同类型的机架：

- 计算
- 边缘
- 基础架构

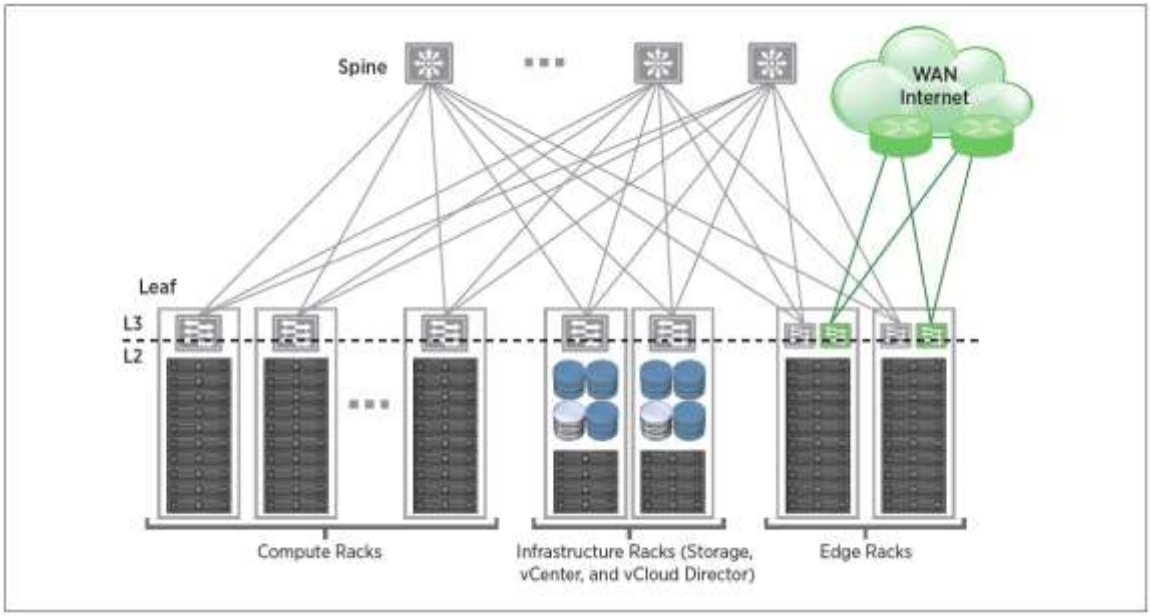

图 12. 数据中心设计 – 访问层中的第 3 层

计算机架

计算机架是基础架构内承载租户虚拟机的部分。它们应该具有以下设计特征：

- 与现有网络互操作
- 对于新部署或重新设计情形
  - 应该不需要对虚拟机使用 VLAN
  - 应该不需要 VLAN 来扩展到计算机架之外
- 提供可重复的机架设计

虚拟化管理程序通常会输出三种或更多种类型的流量。下面我们来了解 VXLAN、管理、vSphere vMotion 和存储流量。VXLAN 流量是一种新型流量，携带所有虚拟机通信数据并将其封装在 UDP 帧中。下面一节将讨论虚拟化管理程序如何连接到外部网络以及通常如何配置这些不同类型的流量。

连接虚拟化管理程序

机架中的服务器通过许多 1 Gb 以太网（1 GbE）接口或数量有限的 10 GbE 接口连接到访问层交换机。服务器物理网卡连接到另一端的虚拟交换机。有关如何将网卡连接到虚拟和物理交换机的最佳实践，请参考《VMware vSphere Distributed Switch 最佳做法技术白皮书》http://www.vmware.com/files/pdf/techpaper/vsphere-distributed-switch-best-practices.pdf。

可以通过 VLAN 将不同的流量类型隔离，从而实现明确的分离以便于进行 IP 寻址。将为各种 VMkernel 网卡分配不同的 VLAN 和 IP 地址。每个 VLAN 都在分支交换机处终止，因此分支交换机将为每个 VLAN 提供第 3 层接口。此类接口也称为 SVI 或 RVI。

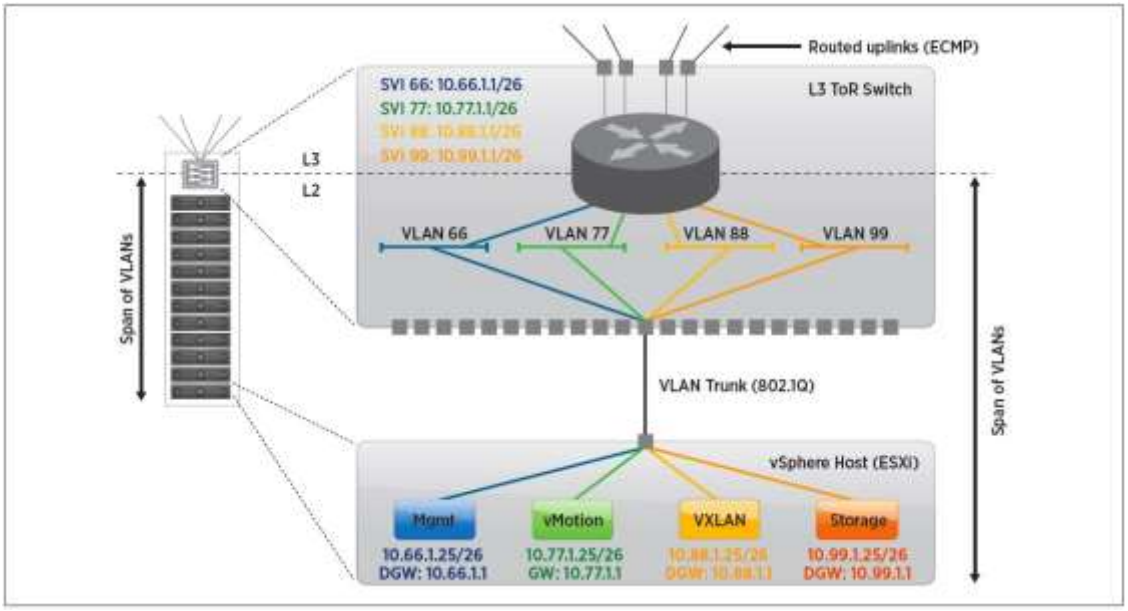

图 13. 示例 – 机架中的主机和分支交换机配置

由于虚拟化管理程序可以有多个路由接口，因此我们将详细介绍如何配置它们。可以通过 DHCP 为不同的 VMkernel 网卡分配不同的网关，或者也可以静态分配 IP 地址。选择静态分配方式时，只能配置一个默认网关。这需要进行静态路由配置，管理网络 VMkernel 网卡不需要静态路由配置，但其他 VMkernel 网卡则需要。

现在，我们来更详细地了解一些主机流量类型：

VXLAN 流量

使用 VXLAN 完成对 vSphere 主机的网络虚拟化准备工作后，在这些主机上将支持一种新的流量类型。连接到基于 VXLAN 的逻辑第 2 层网络之一的虚拟机将使用这种类型的流量进行通信。来自虚拟机的流量将被封装成 VXLAN 流量并发送出去。外部物理结构从不检测虚拟机 IP 和 MAC 地址。将使用虚拟安全加密链路端点（VTEP）IP 地址在结构中传输该帧。如果使用 VXLAN，安全加密链路将由 VTEP 启动和终止。在同一数据中心中的虚拟机之间传输的流量通常称为东西向流量。对于这种类型的流量，源和目标 VTEP 都位于计算机架内的虚拟化管理程序中。例如，离开数据中心的流量将在租户虚拟机和 NSX 边缘之间传输。这种流量称为南北向流量。

VXLAN 配置需要一个 NSX vSwitch。由于 VDS 可以跨越数百个虚拟化管理程序，它可能会延伸到单个分支交换机的范围之外。因此，主机 VTEP 即使处于同一 VDS 上也必须能够位于不同的子网中。基于单个 VDS 的设计的其中一项要求是为 VXLAN 传输网络定义单个 VLAN。

管理流量

管理流量可以分为两种类型：一种流量流入和流出主机上的管理 VMkernel 接口；另一种流量是各种 NSX 组件之间的通信流量。通过主机的管理 VMkernel 接口传送的流量包括 vCenter Server 与主机之间的通信流量以及与其他管理工具（如 NSX Manager）之间的通信流量。NSX 组件之间的通信包括活动和备用边缘设备之间的信号检测。

管理流量只在数据中心内传输。单个 VDS 可以跨在单个分支交换机之外部署的多个虚拟化管理程序。因为没有任何 VLAN 可以超出分支交换机的范围，因此参与通用 VDS 的虚拟化管理程序的管理接口将位于单独的子网中。

vSphere vMotion 流量

在 vSphere vMotion 迁移过程中，正在运行的虚拟机的状态将通过网络传输到另一台主机。将使用每台主机上的 vSphere vMotion VMkernel 接口传输此虚拟机状态。将为主机上的每个 vSphere vMotion VMkernel 接口分配一个 IP 地址。同时进行的虚拟机 vSphere vMotion 迁移操作的数量根据物理网卡的速度决定。在 10 GbE 网卡上，可以同时执行 8 个 vSphere vMotion 迁移操作。为方便支持起见，建议将 VMkernel 接口安排在同一子网中。不过，在使用访问层中的第 3 层为实施网络虚拟化而设计网络时，用户可以为 vSphere vMotion VMkernel 接口选择不同机架中的不同子网。对于日常支持，建议用户遵循 RPQ 过程，以便 VMware 验证设计。

除非涉及到跨不同站点的远距离 vSphere vMotion 迁移，否则 vSphere vMotion 流量主要存在于数据中心内。与管理 VMkernel 接口一样，根据主机所在的机架，该主机上的 vSphere vMotion VMkernel 接口将位于单独的子网中。

存储流量

VMkernel 接口用于提供共享或非直连式存储等功能。通常，我们是指存储可以通过 IP 连接（例如，NAS 或 iSCSI）而非 FC 或 FCoE 进行连接。从 IP 寻址的角度看，适用于管理流量的规则也适用于存储 VMkernel 接口。机架内的服务器的存储 VMkernel 接口（即，连接到分支交换机的接口）属于同一子网。不过此子网不能超出此分支交换机的范围。因此，位于不同机架中的主机的存储 VMkernel 接口 IP 将位于不同的子网中。有关这些 VMkernel 接口的 IP 地址的示例，请参见“VLAN 配置”一节。

边缘机架

在覆盖环境和物理基础架构之间进行桥接时，将加强与物理基础架构的交互。下面是边缘机架提供的主要功能：

- 提供与物理网络的传入和传出连接
- 与物理环境中的 VLAN 连接
- 承载集中式物理服务

如果流量没有封装在 VXLAN 中（例如，没有在边缘使用 NAT），租户特定的寻址将向物理基础架构公开。如果是第 3 层边缘，覆盖环境中的 IP 地址将向物理结构公开。这些情况下的指导原则是将 VXLAN（覆盖）流量与未封装（本机）流量分隔开。如图 14 所示，VXLAN 流量到达数据中心内部以太网交换基础架构。本机流量遍历面向 WAN 或 Internet 的专用交换和路由基础架构，并与数据中心内部网络完全分离。

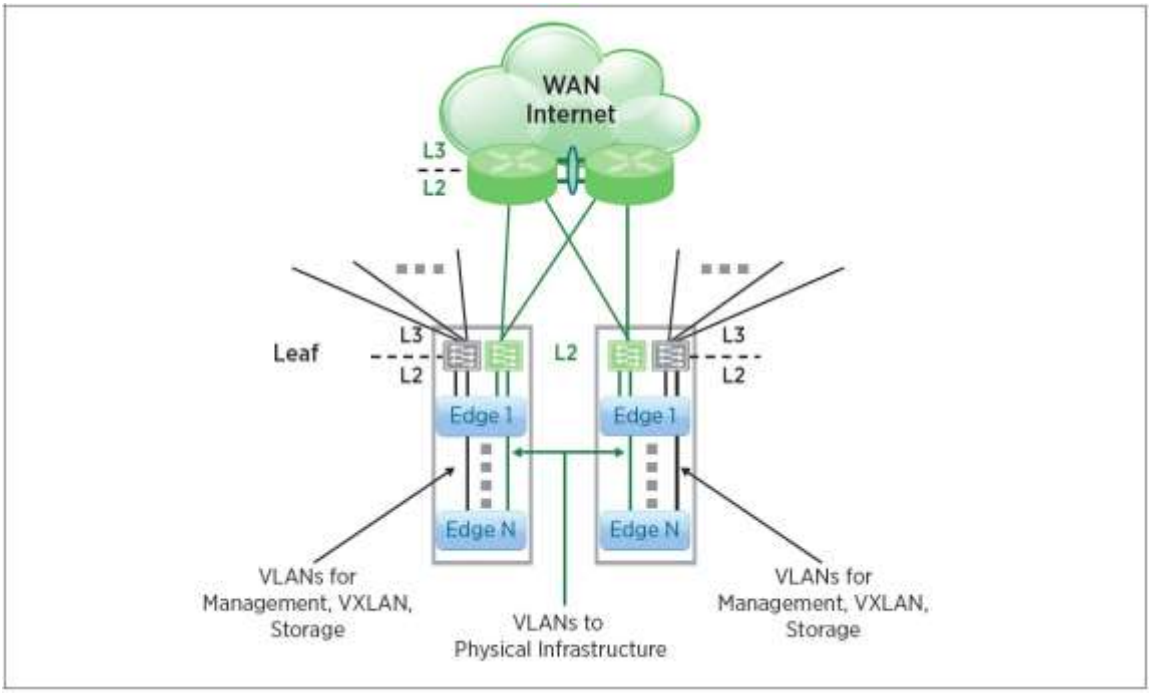

图 14. VXLAN 流量和数据中心内部以太网交换基础架构

为了保持隔离，可以将 NSX Edge 虚拟机放置在边缘机架中，并假定 NSX Edge 至少有一个本机接口。为了实现路由和高可用性，必须分别检查两种类型的接口：覆盖和本机。故障切换机制基于“活动-备用”模型，在检测到活动边缘故障后，备用边缘将接管活动边缘。

第 3 层边缘

在此情况下，边缘会终止所有逻辑网络并在物理和逻辑环境之间提供一个第 3 层跃点。根据具体使用情形，用户可以决定采用 NAT 还是静态路由选项来提供与外部网络的连接。

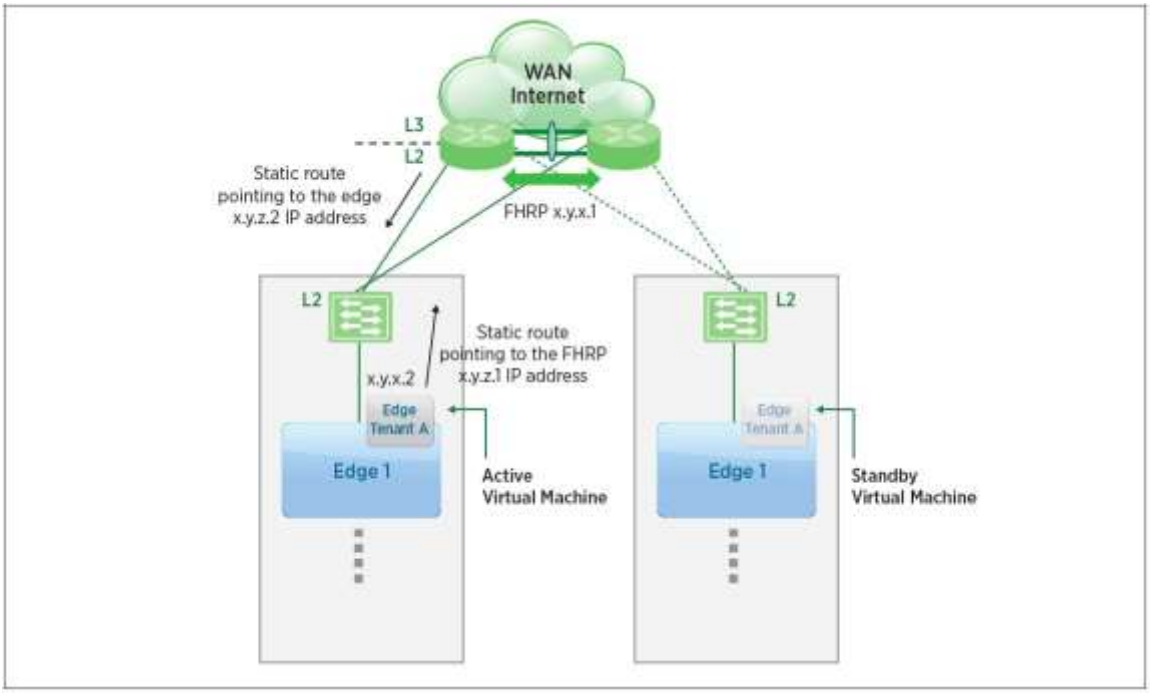

图 15. 高可用性 – “活动-备用”边缘拓扑

如果边缘发生故障，备用边缘将接管故障边缘，并采用以前的活动边缘的外部 IP 地址。为了通知上游基础架构（即，可能会使边缘和第一个物理路由器相互连接的第 2 层交换机），将发送一条 GARP 消息。若要让该机制发挥作用，VLAN 必须在边缘机架之间扩展。连接 VXLAN 端点的安全加密链路接口不必扩展任何 VLAN。故障切换前，虚拟化管理程序的 VTEP 将流量发送至承载该边缘的虚拟化管理程序的 VTEP。故障切换后，该流量将发送至承载新的活动边缘的虚拟化管理程序的 VTEP。

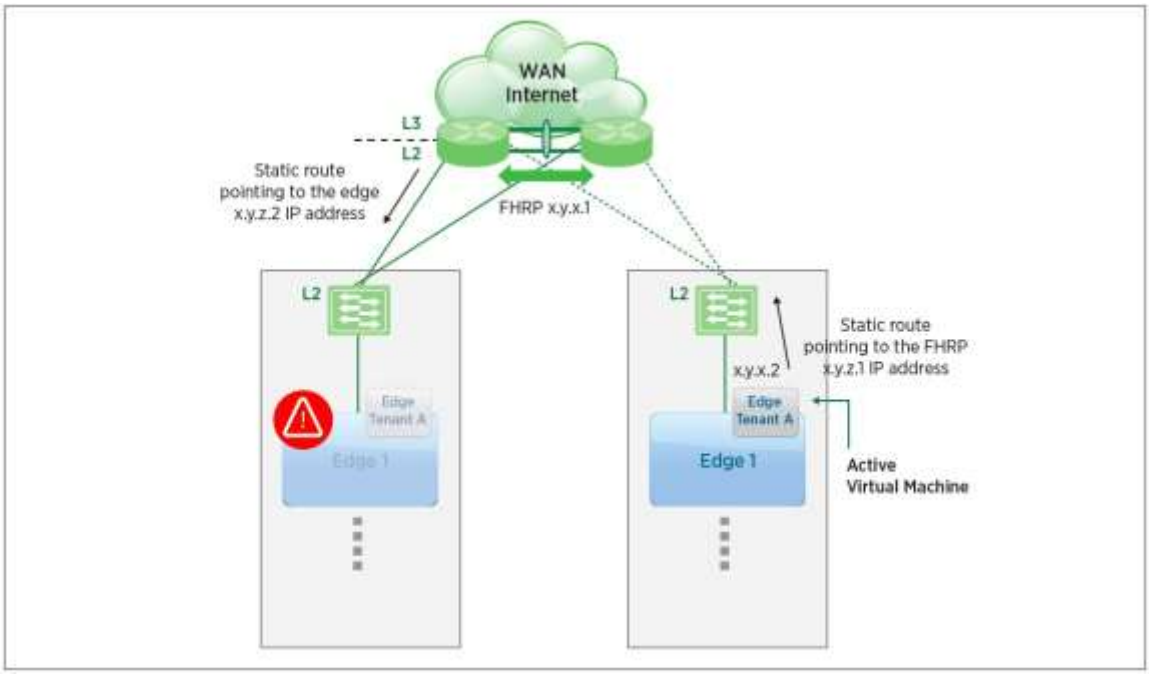

图 16. 活动边缘故障

基础架构机架

基础架构机架承载管理组件，包括 vCenter Server、NSX Manager、NSX Controller、CMP 和其他与共享 IP 存储相关的组件。基础架构的这一部分不包含任何租户特定的寻址，这一点非常重要。如果带宽密集型基础架构服务（例如，基于 IP 的存储）位于这些机架中，这些机架的带宽将可以动态扩展，如“**数据中心结构属性**”一节的“**高带宽**”小节所述。

VLAN 配置

正如前面所述，每个计算机架都有四个不同的子网来分别支持四种不同类型的流量：租户、管理、vSphere vMotion 和存储流量。在本节中，我们将讨论如何使用 vSphere 主机配置文件方法自动完成向每种流量类型的 VMkernel 网卡配置 IP 地址的过程。
用户可以使用主机配置文件功能来创建一个参考主机，它具有在整个部署中共享的属性。确定该主机并执行所需的示例配置后，即可基于该主机创建主机配置文件并将其应用于部署中的其他主机。使用这种方法，用户可以快速配置大量主机。

在讨论如何在配置整个计算机架期间使用主机配置文件方法之前，我们先了解一下机架中的主机上所需的示例配置类型。如图 17 所示，每个机架中都提供同一组 VLAN（4 个）：存储、vSphere vMotion、VXLAN、管理。下面是每台主机所需的部分配置：

1) 相应子网或 VLAN 中每种流量类型的 vmknic IP 配置
2) 每个子网的静态路由配置，用于处理路由到相应网关的适当流量

静态路由是必需的，因为 VMware ESXi™ 主机上的一个 TCP 或 IP 堆栈支持会将默认网关配置数量限制为一个。

例如，在机架 1 中，主机 1 具有以下 vmknic 配置：

- IP 地址为 10.66.1.10 的存储 vmknic
- IP 地址为 10.77.1.10 的 vSphere vMotion vmknic
- IP 地址为 10.88.1.10 的 VXLAN vmknic
- IP 地址为 10.99.1.10 的管理 vmknic

主机 1 上的默认网关配置位于管理 vmknic 子网 10.99.1.0/26 中。为了向其他子网提供适当路由支持，将在准备主机 1 的过程中配置以下静态路由：

- 存储网络路由 – esxcli network ip route ipv4 add -n 10.66.0.0/26 -g 10.66.1.1
- vSphere vMotion 网络路由 – esxcli network ip route ipv4 add -n 10.77.0.0/26 -g 10.77.1.1

配置完机架 1 的主机 1 后，将创建一个主机配置文件，随后将此配置文件应用于机架中的其他主机。将配置文件应用于主机后，将创建新 vmknic 并添加静态路由，以简化部署。

在 vSphere Auto Deploy 环境中，PXE 引导基础架构连同 Auto Deploy 服务器和 vCenter Server 支持主机引导过程，并帮助自动执行 ESXi 主机的部署和升级。

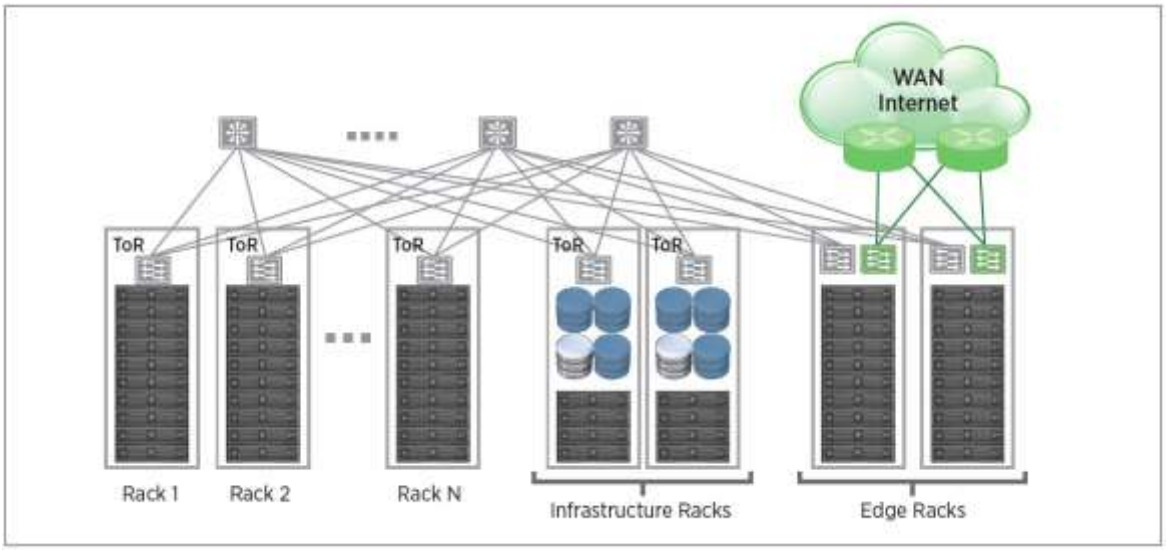

图 17. 主机基础架构流量类型和 IP 地址分配

IP ADDRESS MANAGEMENT AND VLANs[1]		
Function	**Global VLAN ID**	**IP Address**
Storage	66	10.66.R_id.x/26
vMotion	77	10.77.R_id.x/26
VXLAN/VTEP	88	10.88.R_id.x/26
Management	99	10.99.R_id.x/26

[1] Values of VLANs, IP addresses, and masks are an example (not prescriptive to the design)

表 1. IP 地址管理和 VLAN

多层边缘和多层应用设计注意事项

经典的多层计算体系结构具有逻辑上分离的多项功能，每项功能在资源访问、数据分离和安全性方面都有不同的要求。经典的三层体系结构通常包含一个表示层、一个应用或数据访问层和一个数据库层。应允许应用层与数据库层通信，而外部用户只能访问表示层，该层通常是一个基于 Web 的服务。为遵守数据访问策略，建议的解决方案是部署一个包含两层的边缘设计。内部边缘在由不同的逻辑网络表示的表示层、数据库层和应用层之间实现 VXLAN 到 VXLAN 之间的东西向流量。外部边缘将表现层与外部环境相连以提供传入和传出流量。特定虚拟网络内的通信使虚拟机能够跨越多个机架，以实现计算机架基础架构的最佳利用率。在当前阶段，逻辑网络只能跨单个 vCenter 域。图 18 显示了此体系结构的逻辑元素的位置。

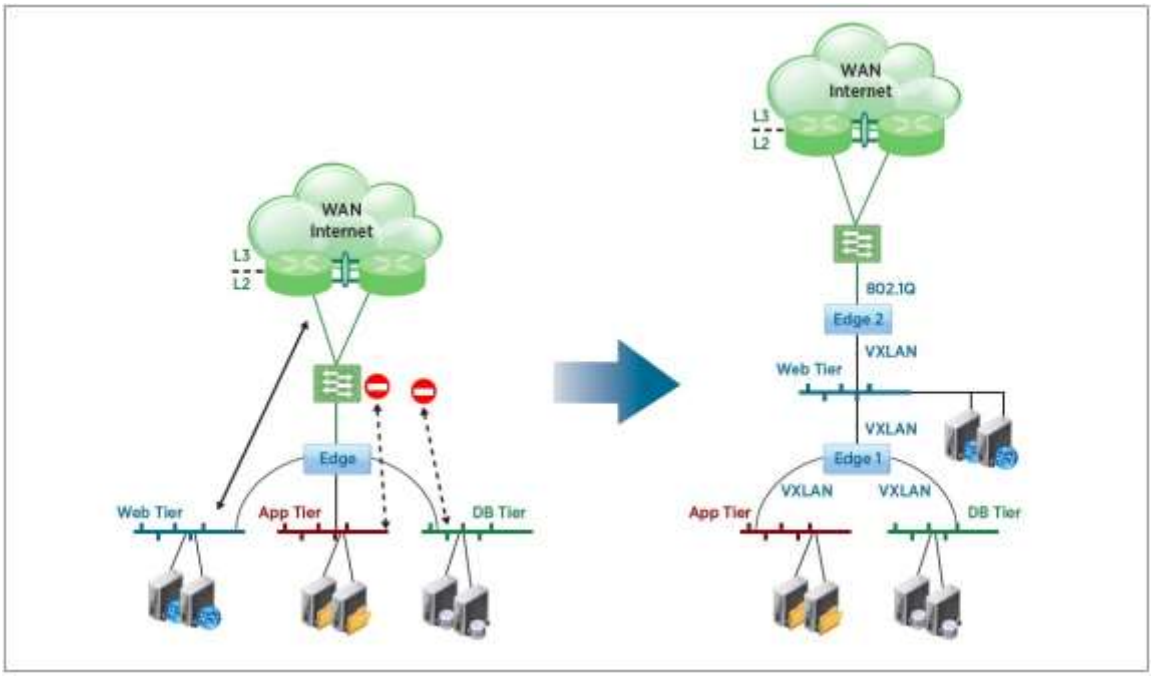

图 18. 多层应用中逻辑元素位置的两种选项

最好将外部边缘实际放置在边缘机架中。内部边缘可以集中放置在边缘机架中，也可以分布于 Web 和应用计算资源所在的计算机架中。

逻辑交换

NSX 平台中的逻辑交换功使客户能够快速将隔离的逻辑第 2 层网络投入运行，并获得相同的灵活性和敏捷性，因为它是要将虚拟机快速投入运行。本节介绍逻辑交换中的各个组件以及这些组件之间的通信。

组件

如图 19 所示，有三个主要组件可帮助分离底层物理网络结构并提供网络抽象化。用更具技术性的话来说，这种分离是通过使用 VXLAN 或 STT 协议封装虚拟机流量来实现的。我们来看一下逻辑交换中使用的每个组件的功能。

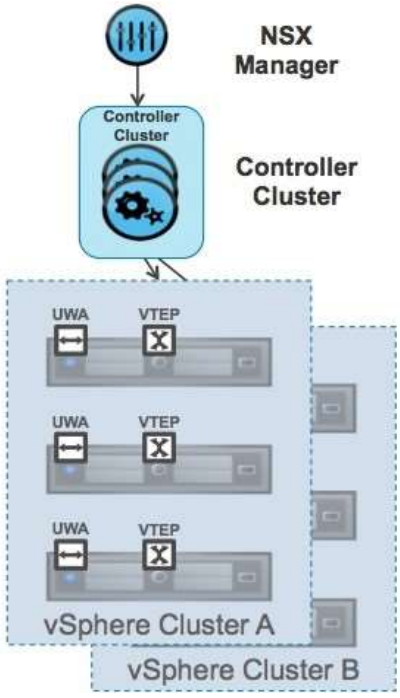

图 19.逻辑交换组件

NSX Manager

NSX Manager 是管理板组件，可帮助配置逻辑交换机并将虚拟机连接到这些逻辑交换机。它还提供 API 接口，帮助通过云管理平台实现这些交换机的部署和管理自动化。

控制器集群

NSX 平台中的控制器集群是控制板组件，它负责管理虚拟化管理程序中的交换和路由模块。控制器集群由管理特定逻辑交换机的控制器节点组成。使用控制器集群来管理基于 VXLAN 的逻辑交换机，就不再需要物理网络基础架构提供多播支持。现在，客户不必配置多播组 IP 地址，也不需要在物理交换机或路由器上启用 PIM 路由或 IGMP 监听功能。创建逻辑交换机时选中“Unicast”（单播）复选框可启用此 VXLAN 操作模式。

用户环境代理 (UWA) 和 VXLAN 安全加密链路端点 (VTEP)

虚拟化管理程序上有两个数据板组件，用于在控制器集群和其他虚拟化管理程序之间提供通信路径。它们还执行逻辑交换机的数据路径功能。

用户环境代理用于与控制器集群建立通信，而VTEP 提供在虚拟化管理程序之间创建安全加密链路的功能。

在准备过程中，将通过 NSX Manager 部署和配置控制器集群和虚拟化管理程序模块。配置逻辑交换组件后，下一步是定义逻辑交换机的范围。逻辑交换机的范围通过创建传输区域定义。在传输区域中，客户可以添加一组集群。例如，如果数据中心中有 10 个集群，传输区域可以包含所有这 10 个集群。在这样的情况下，逻辑交换机可以跨越整个数据中心。下图显示了安装 NSX 组件以提供逻辑交换后的部署。边缘机架中的 Edge 服务路由器提供对 WAN 和其他网络服务的逻辑交换机访问。

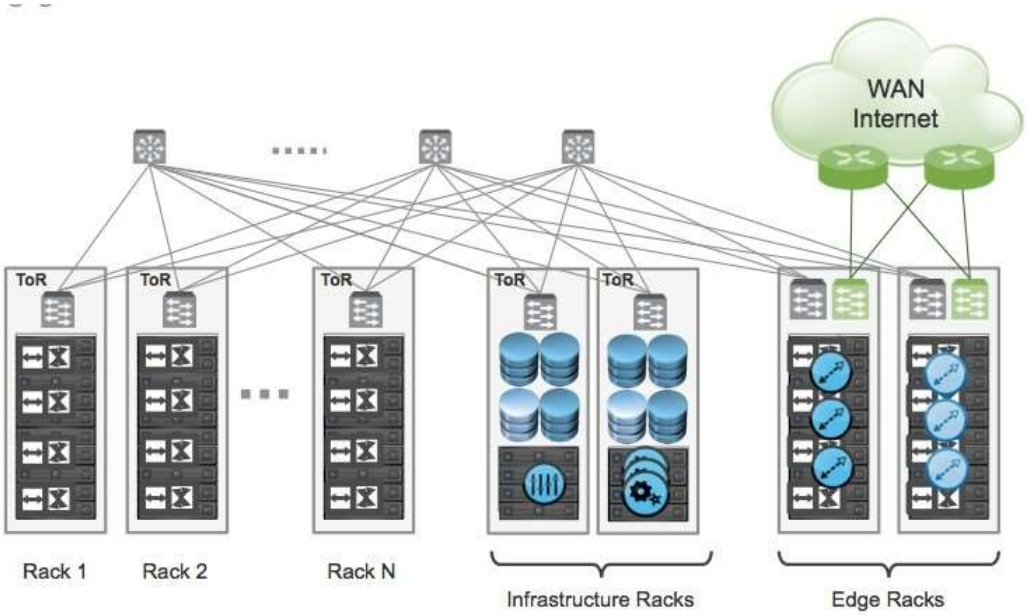

图 20. 机架中的逻辑交换组件

逻辑交换寻址

在具有多个租户的大型云环境或具有多个组织和应用的大企业中，IP 地址管理是一项关键任务。在本节中我们将重点介绍对逻辑交换机上部署的虚拟机的 IP 地址管理。创建的每个逻辑交换机都是一个单独的第 2 层广播域，它可以使用专用 IP 空间或公共 IP 空间与一个单独的子网相关联。根据是使用专用 IP 空间还是公共 IP 空间向逻辑网络分配地址，用户必须在 NSX Edge 服务路由器上选择使用 NAT 还是非 NAT 选项。因此，IP 地址分配取决于虚拟机是通过 NAT 还是非 NAT 配置连接到逻辑交换机。我们将分别查看下面两种部署的示例：

1) 使用 Edge 服务路由器的 NAT 服务
2) 不使用 Edge 服务路由器的 NAT 服务

使用网络地址转换

在组织的 IP 地址空间有限的部署中，将使用 NAT 来提供从专用 IP 空间到有限的公共 IP 地址的地址转换。通过利用 Edge 服务路由器，用户可允许各个租户创建他们自己的专用 IP 地址池，这些地址最终将映射到 Edge 服务路由器外部接口的可公开路由的外部 IP 地址。

图 21 显示了一个三层应用部署，其中每一层的虚拟机都连接到单独的逻辑交换机。Web、应用和数据库逻辑交换机连接到 Edge 服务路由器的三个内部接口；Edge 服务路由器的外部接口通过外部数据中心路由器连接到 Internet。

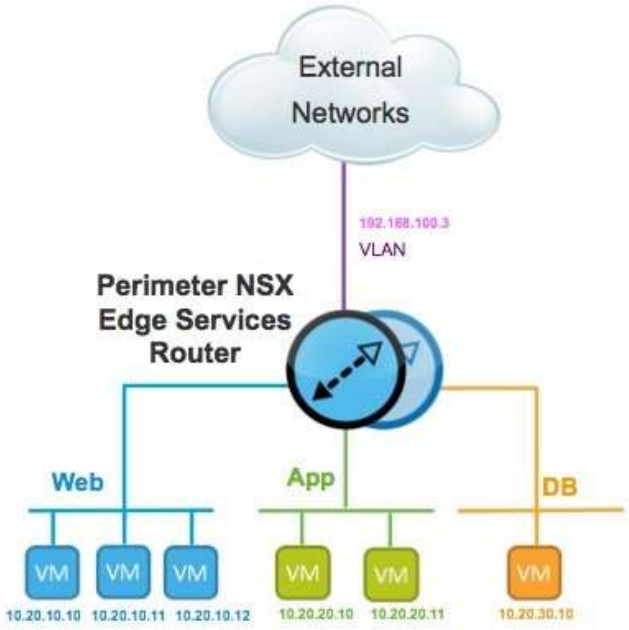

图 21.NSX Edge 服务路由器上的 NAT 和 DHCP 配置

下面是 NSX Edge 服务路由器的配置详情：

- Web、应用和数据库逻辑交换机连接到 NSX Edge 服务路由器的内部接口。
- NSX Edge 服务路由器的上行链路接口连接到位于子网 192.168.100.0/24 内的 VLAN 端口组。
- 通过提供 IP 地址池在该内部接口上启用 DHCP 服务例如，10.20:10.10 到 10.20:10.50。
- vCloud Networking and Security Edge 网关的外部接口上的 NAT 配置使逻辑交换机上的虚拟机能够与外部网络中的设备通信。仅当请求是由连接到 Edge 服务路由器的内部接口的虚拟机发起时，才允许这种通信。

如果需要支持重叠 IP 和 MAC 地址，则建议对每个租户使用一个 Edge 服务路由器。图 22 显示了具有两个租户和两个单独的 NSX Edge 服务路由器的重叠 IP 地址部署。

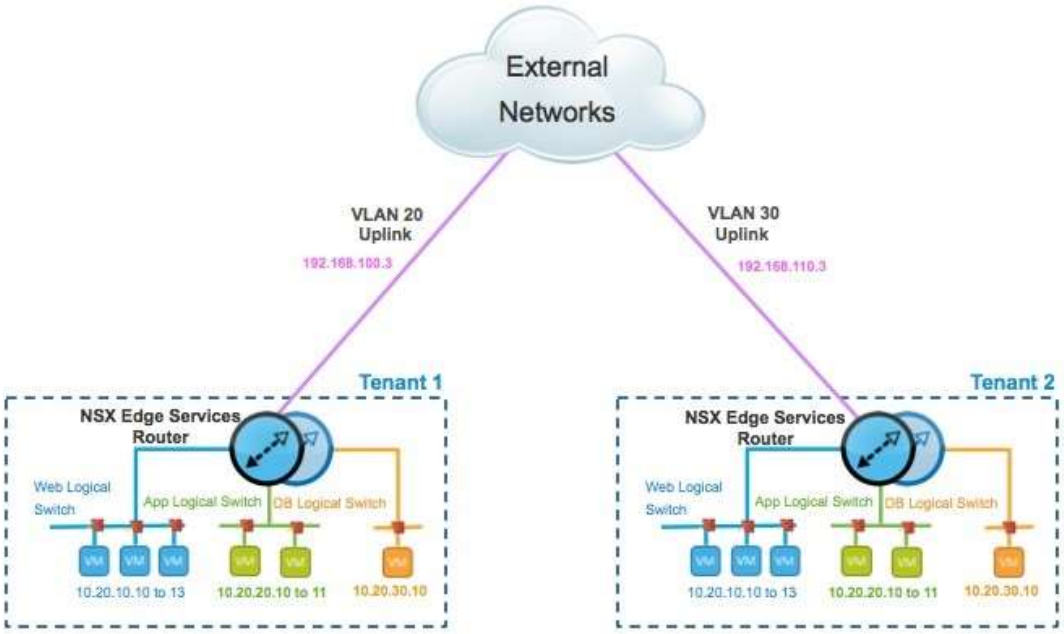

图 22.重叠 IP 和 MAC 地址

不使用网络地址转换

不受可路由 IP 地址限制的组织、有虚拟机使用公共 IP 地址的组织或者不想部署 NAT 的组织可以使用 NSX 平台提供的静态和动态路由功能。在 NSX 平台中支持两种不同模式的逻辑路由。一种称为分布式路由，另一种称为集中式路由。分布式路由为东西向流量提供更高的吞吐量和性能，而集中式路由则处理南北向流量。下面一节提供有关逻辑路由的更多详细信息。有关数据中心中的应用所需的更多网络服务，请参见“逻辑防火墙”和“逻辑负载平衡器”两节。

逻辑路由

如前面一节所述，NSX 平台支持两种模式的路由。本节将详细介绍这两种模式，同时还介绍客户环境中可以构建的一些常见路由拓扑。

分布式路由

NSX 平台中的分布式路由功能提供一种经过优化且可扩展的方法来处理数据中心内的东西向流量。数据中心内的虚拟机或资源之间的通信称为东西向流量。数据中心中东西向流量正在不断增多。新的协作式、分布式且面向服务的应用体系结构需要更高的带宽来实现服务器之间的相互通信。

如果这些服务器是运行在虚拟化管理程序上的虚拟机，并且它们连接到不同的子网，那么这些服务器之间的通信流量必须经过路由器。同样，如果使用物理路由器来提供路由服务，那么虚拟机通信信息必须先传出到物理路由器，然后在收到路由决定后再返回到服务器。这种非最佳方式的通信流有时称为“发夹”。

NSX 平台上的分布式路由可通过提供虚拟化管理程序级别的路由功能来防止出现“发夹”。每个虚拟化管理程序都有一个路由内核模块，在该分布式路由器实例上定义的逻辑接口（LIF）之间执行路由。下面的“组件”一节介绍分布式路由中的各个模块以及这些模块之间的通信。

集中式路由

NSX Edge 服务路由器在 NSX 平台中提供传统的集中式路由支持。除路由服务外，NSX Edge 还支持其他网络服务，其中包括 DHCP、NAT、负载平衡等。

组件

如图 23 所示，逻辑路由有多个组件。有些组件与分布式路由相关，有些则与集中式路由相关。我们来看一下每个组件及其在分布式或集中式路由中的功能。

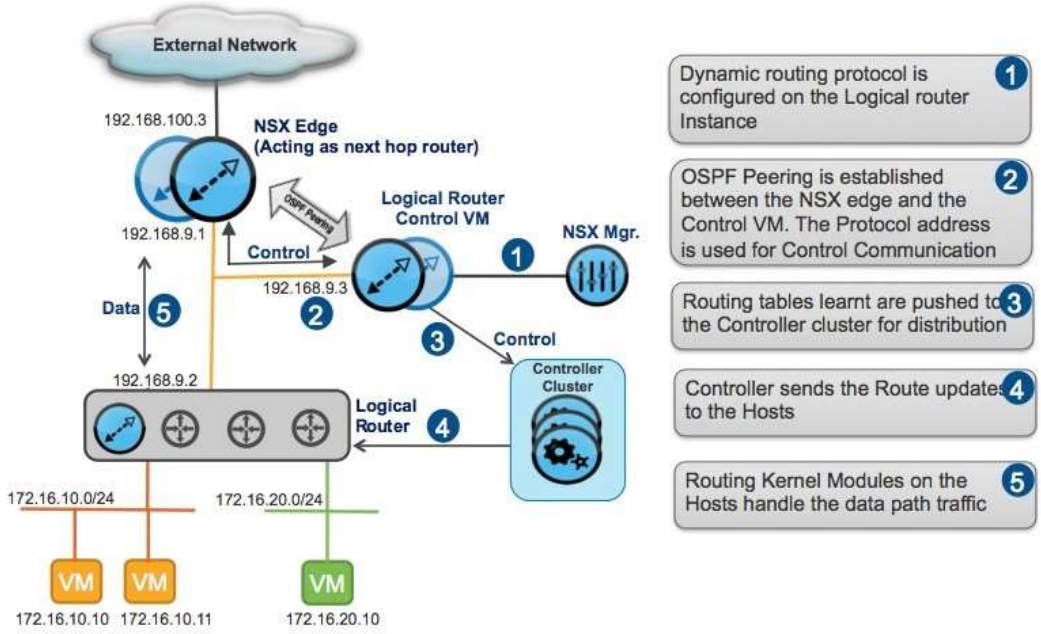

图 23. 逻辑路由组件

NSX Manager

NSX Manager 还帮助配置和管理逻辑路由服务。在配置过程中，客户可以选择部署分布式或集中式逻辑路由器。如果选择分布式路由器，NSX Manager 将部署逻辑路由器控制虚拟机并通过控制器集群将逻辑接口配置推送到每台主机。如果选择集中式路由，NSX Manager 只部署 NSX Edge 服务路由器虚拟机。NSX Manager 的 API 接口可通过云管理平台帮助自动完成这些逻辑路由器的部署和管理。

逻辑路由器控制虚拟机

逻辑路由器控制虚拟机是路由过程的控制板组件。它支持以下动态路由协议：

1) OSPF
2) BGP

逻辑路由器控制虚拟机使用动态路由协议与下一跃点路由器通信，并通过控制器集群将获得的路由推送给虚拟化管理程序。客户可以在部署控制虚拟机的同时实现高可用性 (HA)。当选择 HA 模式时，将会有两台虚拟机以“活动-备用”模式部署。

逻辑路由器内核模块

逻辑路由器内核模块在准备过程中通过 NSX Manager 配置。内核模块与支持第 3 层路由的模块化机架中的线卡类似。内核模块具有通过控制器集群推送的路由信息库 (RIB)。路由查找、ARP 条目查找的所有数据板功能均由内核模块执行。

控制器集群

控制器集群负责在虚拟化管理程序之间分发从控制虚拟机获得的路由。该集群中的每个控制器节点负责分发某特定逻辑路由器实例的信息。在部署了多个逻辑路由器实例的部署中，负载将在多个控制器节点之间分配。

NSX Edge 服务路由器

这是一种集中式服务路由器，可提供其他网络服务并支持以下路由协议：

1) BGP
2) OSPF
3) IS-IS

此处所说的其他服务包括 DHCP、NAT、防火墙、负载平衡和 VPN 功能。

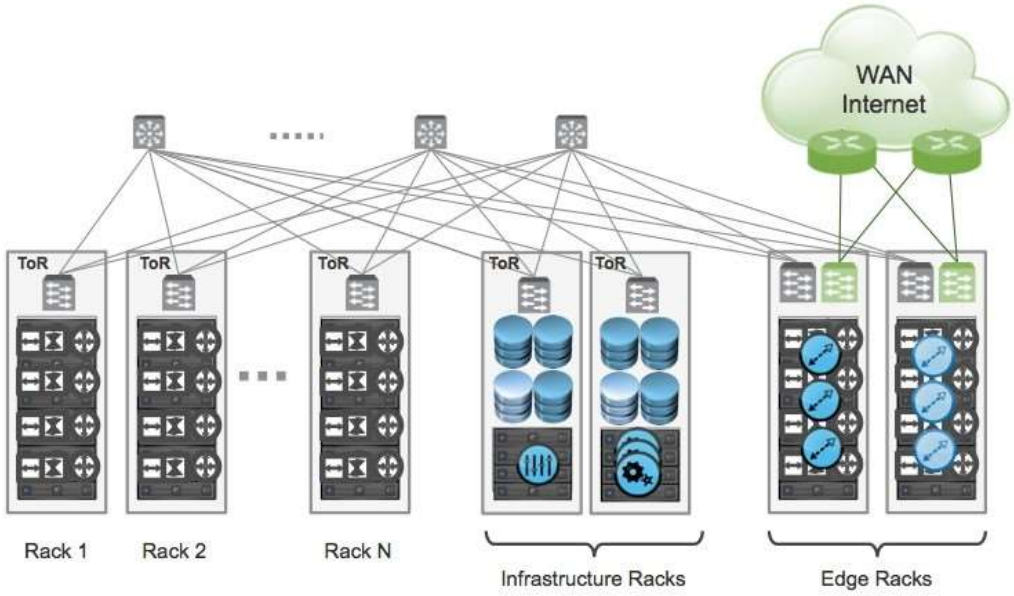

图 24. 机架中的逻辑路由组件

路由部署

根据客户要求，可以使用 NSX 平台的逻辑交换和逻辑路由功能来构建多个拓扑。本节中我们将讨论下面两种路由拓扑，它们同时利用分布式和集中式逻辑路由功能：

1) 用作下一跃点的物理路由器
2) 用作下一跃点的 Edge 服务路由器

用作下一跃点的物理路由器

如下图所示，一个组织托管多个应用，并希望在不同的应用层之间提供连接，同时还希望能够连接到外部网络。在该拓扑中，由单独的逻辑交换机为特定层中的虚拟机提供第 2 层网络连接。分布式逻辑路由配置允许两个不同层上的虚拟机相互通信。同样，逻辑路由器上的动态路由协议支持允许与下一跃点物理路由器交换路由。这进而使外部用户能够访问连接到数据中心中的逻辑交换机的应用。

在这种拓扑中，东西向和南北向路由决策以分布式方式在虚拟化管理程序级别做出。

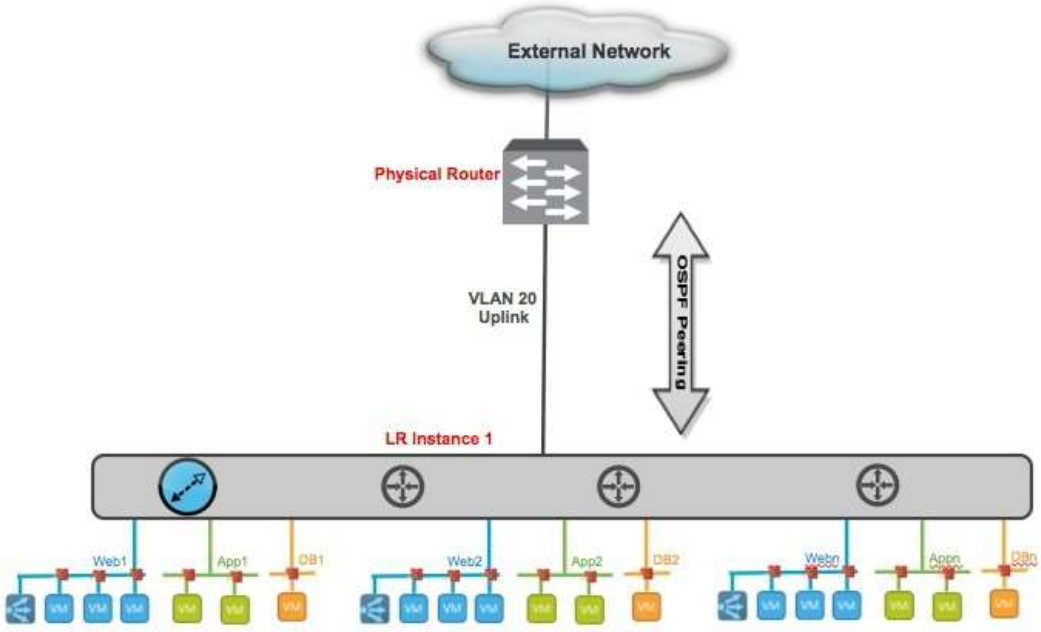

图 25. 用作下一跃点的物理路由器

用作下一跃点的 Edge 服务路由器

在存在多个租户的服务提供商环境中，每个租户对隔离的逻辑网络和其他网络服务（如负载平衡、防火墙和 VPN 等）的数量可能有不同的要求。在此类部署中，NSX Edge 服务路由器可提供网络服务功能以及动态路由协议支持。

如下图所示，两个租户通过 NSX Edge 服务路由器连接到外部网络。每个租户都有各自的逻辑路由器实例在租户内提供路由功能。此外，租户的逻辑路由器与 NSX Edge 服务路由器之间的动态路由协议配置允许租户虚拟机连接到外部网络。

在这种拓扑中，东西向流量路由通过虚拟化管理程序中的分布式路由器处理，南北向流量则流经 NSX Edge 服务路由器。

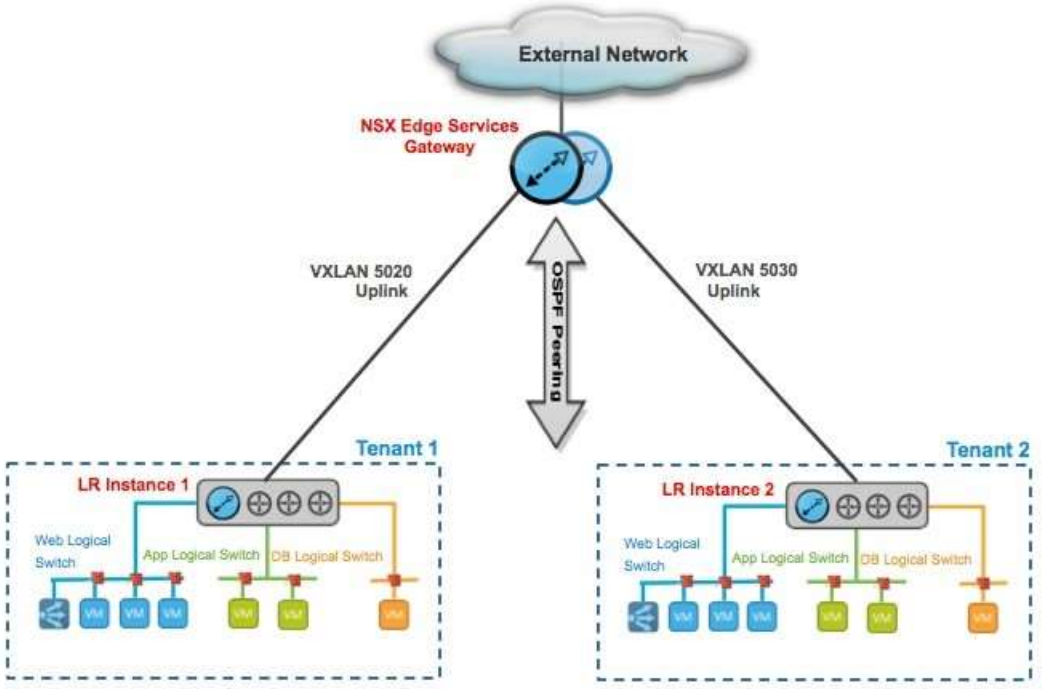

图 26. NSX Edge 服务路由器用作下一跃点，并且还提供网络服务

可扩展拓扑

前面一节中描述的服务提供商拓扑可以如图 27 所示进行横向扩展。该图左侧显示由 NSX Edge 提供服务的九个租户，右侧显示由 Edge 提供服务的另外九个租户。服务提供商可以轻松地再调配一个 NSX Edge 来为更多租户提供服务。

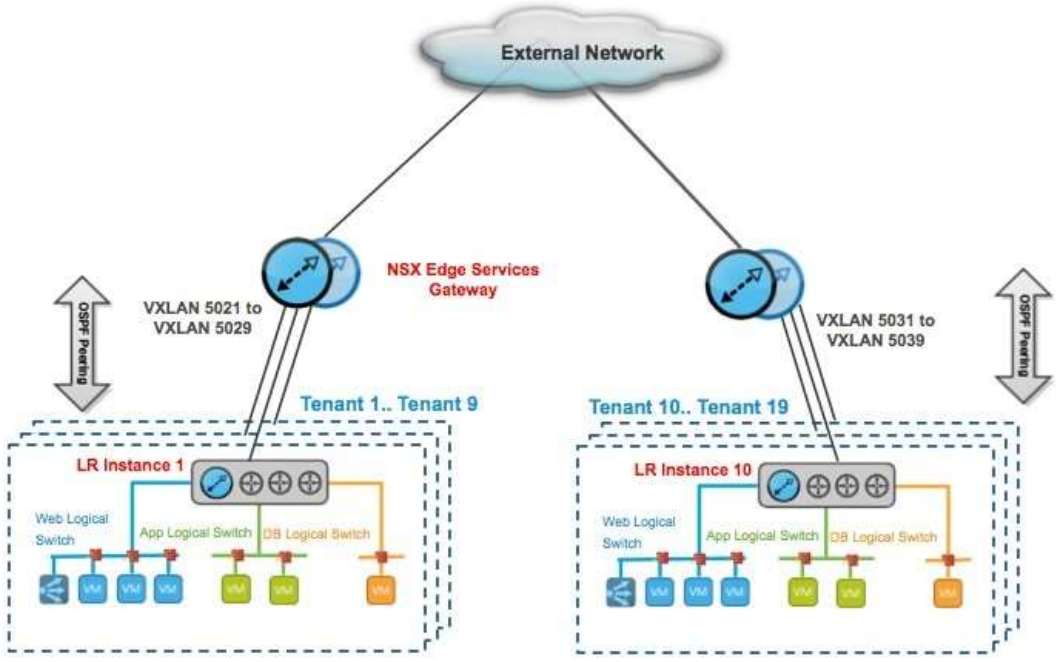

图 27. 可扩展拓扑

逻辑防火墙

除网络虚拟化固有的其他网络安全功能外，VMware NSX 平台还包含支持分布式内核、具有线速性能、可识别虚拟化和身份并且能够监控活动的防火墙。

网络隔离

隔离是大多数网络安全的基础，无论是为了实现合规性、数据控制，还是只是为了防止开发、测试和生产环境进行交互，隔离都必不可少。虽然过去使用物理设备上手动配置和维护的路由、ACL 和/或防火墙规则来建立和强制实施隔离，但现在实现网络虚拟化后，隔离和多租户架构已成为固有功能。

虚拟网络彼此隔离，并且默认情况下与底层物理网络隔离，从而实现最少特权安全原则。除非专门将虚拟网络连接在一起，否则它们以隔离方式创建并且始终保持隔离状态。不需要物理子网、VLAN、ACL 和防火墙规则，即可实现这种隔离。

任何隔离的虚拟网络均可以由分布在数据中心中的任何位置的工作负载组成。同一虚拟网络中的工作负载可以驻留在相同或不同虚拟化管理程序中。此外，多个隔离的虚拟网络中的工作负载也可以驻留在同一虚拟化管理程序中。例如，虚拟网络之间的隔离允许重叠的 IP 地址，从而能够实现相互隔离的开发、测试和生产虚拟网络，每个网络都包含不同的应用版本，但却拥有相同的 IP 地址，所有网络均可同时运行，并且全部位于同一底层物理基础架构中。

虚拟网络还将与底层物理基础架构隔离。由于虚拟化管理程序之间的流量是封装的，因此运行物理网络设备的地址空间与工作负载用于连接到虚拟网络的地址空间完全不同。例如，虚拟网络可以基于 IPv4 物理网络支持 IPv6 应用工作负载。这种隔离可以帮助基础物理基础架构抵御由任何虚拟网络中的工作负载发起的任何可能的攻击。此外还不依赖于过去创建这种隔离所需的任何 VLAN、ACL 或防火墙规则。

网络分段

通过网络虚拟化可轻松进行分段。分段与隔离相关，但是应用于多层虚拟网络。过去，网络分段是物理防火墙或路由器的一项功能，旨在允许或拒绝网络分段或层之间的流量。例如，对 Web 层、应用层和数据库层之间的流量进行分段。过去定义和配置分段的过程非常耗时，而且极易出现人为错误，从而导致大量安全违规情况。实施过程需要对设备配置语法、网络寻址、应用端口和协议具有精到、专门的专业技能。

与隔离一样，网络分段也是 VMware NSX 网络虚拟化的一项核心功能。虚拟网络可以支持多层网络环境，这意味着多个第 2 层网段（每个第 2 层网段上有第 3 层分段或微分段）可以使用分布式防火墙规则。如上面的示例中所示，这些层可以表示 Web 层、应用层和数据库层。物理防火墙和访问控制列表可提供成熟的、受网络安全团队和合规性审核员信任的分段功能。不过，人们对在云数据中心中采用这种方法的信心已经动摇，因为越来越多的攻击、违规和停机都是由于过时的手动网络安全调配和变更管理流程中的人为错误引起的。

在虚拟网络中，配备有工作负载的网络服务（L2、L3、ACL、防火墙、QoS 等）以编程方式创建并分发给虚拟化管理程序虚拟交换机。包括第 3 层分段和防火墙在内的网络服务在虚拟接口中实施。虚拟网络内的通信绝不会离开虚拟环境，因此无需在物理网络或防火墙中配置和维护网络分段。

利用抽象化处理

过去，网络安全要求安全团队深入了解网络寻址、应用端口、协议、与网络硬件相关的所有信息、工作负载位置和拓扑。网络虚拟化可基于物理网络硬件和拓扑对应用工作负载通信进行抽象化处理，使网络安全摆脱这些物理约束，并根据用户、应用和业务环境应用网络安全。

高级安全服务插入、串联和转向

基础 VMware NSX 网络虚拟化平台提供基本的全状态防火墙功能，以便在虚拟网络内提供分段。在有些环境中，需要更高级的网络安全功能。在这些情况下，客户可以利用 VMware NSX 在虚拟化网络环境中分发、启用和强制实施高级网络安全服务。NSX 将网络服务分发到 vSwitch 中，以形成适用于虚拟网络流量的服务的逻辑管道。可以将第三方网络服务插入此逻辑管道中，从而允许在逻辑管道中使用物理或虚拟服务。

每个安全团队都使用各种网络安全产品的独特组合来满足其环境的需求。VMware 的整个安全解决方案提供商体系都在使用 VMware NSX 平台(http://www.vmware.com/cn/products/nsx/resources.html)。 网络安全团队经常面临协调多个供应商所提供网络安全服务的关系的难题。NSX 方法的另一个巨大好处是它能够构建策略来利用 NSX 服务的插入、串联和转向功能，以便基于其他服务的结果，推动服务在逻辑服务管道中执行，从而能够协调多个供应商提供的本来毫不相关的网络安全服务。

例如，我们与 Palo Alto Networks (http://researchcenter.paloaltonetworks.com/2013/11/palo-alto- networks-vmware-milestone-software-defined-data-center-security/) 的集成将利用 VMware NSX 平台来分发 Palo Alto Networks 虚拟机系列的下一代防火墙，从而在每个虚拟化管理程序本地提供高级功能。为调配或移到该虚拟化管理程序的应用工作负载定义的网络安全策略将插入到虚拟网络的逻辑管道。在运行时，服务插入功能将利用本地提供的 Palo Alto Networks 下一代防火墙功能集，在工作负载虚拟接口交付和强制实施基于应用、用户以及上下文的控制策略。

跨物理和虚拟基础架构的一致的可见性和安全模型

VMware NSX 允许跨虚拟和物理安全平台自动化资源调配和上下文共享。结合虚拟接口处的流量转向和策略实施功能，过去部署在物理网络环境中的合作伙伴服务将可以轻松地在虚拟网络环境中调配和实施，VMware NSX 可以跨驻留在物理或虚拟工作负载中的应用为客户提供一致的可见性和安全性模型。

1. **现有工具和流程。**大幅提高资源调配速度、运营效率和服务质量，同时保持服务器、网络和安全团队的职责分离。
2. **更好地控制应用，没有负面影响。**过去，要达到这种级别的网络安全，网络和安全团队不得不在性能和功能之间做出抉择。现在，利用在应用虚拟接口分发和实施高级功能集的功能可以两全其美。
3. **减少各种操作中的人为错误。**基础架构会维护相应的策略，允许在数据中心中的任何位置放置和移动工作负载，而无需任何人为干预。可以编程方式应用预先批准的应用安全性策略，从而即使对复杂网络安全服务也能实现自助式部署。

逻辑负载平衡

负载平衡是 NSX 中提供的另一项网络服务。

该服务可跨多个服务器**分配工作负载**，并实现**应用的高可用性**：

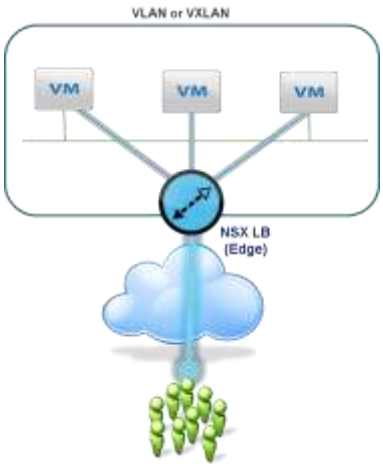

图 28.NSX 负载平衡

NSX 负载平衡服务是专门**针对云计算设计的**，具有以下特点：

- 完全可通过 API 进行编程
- 与其他 NSX 网络服务相同的单个集中管理/监控点

NSX 负载平衡服务具有以下特点，能够满足客户的应用负载平衡需求：

- **多体系结构支持**
  - 单臂模式（称为代理模式）
  - 双臂模式（称为透明模式）

- **大型功能集，可支持大量应用**
  - 支持任何 TCP 应用
  - 包括但不限于 LDAP、FTP、HTTP、HTTPS
  - 多种负载平衡分配算法
  - 循环、最少连接数、源 IP 地址散列、URI
  - 多种运行状况检查
  - TCP、HTTP、HTTPS，包括内容检查
  - 持久性
  - 源 IP、MSRDP、Cookie、SSL 会话 ID
  - 连接调节
  - 最大连接数和每秒连接数
  - 第 7 层操纵
  - 包括但不限于 URL 阻止、URL 重写、内容重写
  - 优化
  - SSL 负载分流

NSX 负载平衡服务**扩展能力非常强，可支持要求非常严苛的应用。**每个 NSX Edge 均可扩展至：

- 吞吐量：9 Gbps
- 并发连接数：100 万

- 每秒新连接数：13.1 万

总结

VMware 网络虚拟化解决方案可解决物理网络基础架构当前面临的挑战，并通过基于 VXLAN 的逻辑网络实现灵活性、敏捷性和可扩展性。除了使用 VXLAN 创建按需逻辑网络的功能外，vCloud Networking and Security Edge 网关还可帮助用户在这些网络上部署各种逻辑网络服务，例如防火墙、DHCP、NAT 和负载平衡。这是因为它能够将虚拟网络与物理网络分离，然后在虚拟环境中重现相关属性和服务。

参考资料

[1] VMware vSphere 5.5 的新增功能
http://www.vmware.com/files/pdf/vsphere/VMware-vSphere-Platform-Whats-New.pdf

[2] vSphere 5.5 的配置上限
http://www.vmware.com/pdf/vsphere5/r55/vsphere-55-configuration-maximums.pdf

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
威睿信息技术（中国）有限公司
中国北京海淀区科学院南路 2 号融科资讯中心 C 座南楼 3 层 邮编：100190 电话：+86-10-5993-4200
中国上海办公室 上海市淮海中路 333 号瑞安广场 15 楼 1501 室 邮编：200021 电话：+86-21-6034-9200
中国广州办公室 广州市天河北路 233 号中信广场 7401 室 邮编：510613 电话：+86-20-3877-1938
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真 852-3696 6101
www.vmware.com/cn

项目号：VMW-NSX-NTWK-VIRT-DESN-GUIDE-V2-101