指南

Cisco Nexus 9000 系列交换机在中小型商业数据中心的入门级部署

Carly Stoughton

2014 年 11 月

目录

简介

概述

Cisco Nexus® 9000 系列交换机产品使任何规模的客户都能享受到下一代数据中心交换功能的优势。本白皮书主要面向从未使用过 Cisco Nexus 9000 系列交换机，但希望了解如何将这些交换机轻松部署在其数据中心的商业客户。

本白皮书重点介绍了 Cisco Nexus 9000 系列交换机的优势，概述了适合中小型客户部署的几种设计，讨论了与现有网络的集成，并介绍了经过思科验证的适用于 Cisco Nexus 9000 系列交换机的拓扑，同时也列举了一些配置示例。

这些极具特色的设计既适用于初次使用 Cisco Nexus 9000 系列交换机的组织，也适用于正在横向扩展数据中心的现有客户组织或成长型组织。上述配置示例将逻辑设计转变成易于使用的有形模板，对于 IT 员工人数不多或日益增加的组织来说，这些模板可简化部署和运营。

您可以选择从初学者的角度了解如何开始使用 Cisco NX-OS 拥有的许多强大的可编程功能，只需参阅本文档末尾部分的“附录 A：自动化和可编程性”即可。本白皮书还提供了许多重要的链接，通过访问这些链接，您可以进一步阅读关于所述的协议、解决方案和设计的信息。对 Cisco Nexus 9000 系列交换机可编程功能的全面讨论不属于本文档的讨论范围。

免责声明

如需获得有关软件版本、支持的最大配置规模和设备规格的最新信息，请随时参阅思科网站 http://www.cisco.com/go/nexus9000。

为什么选择 Cisco Nexus 9000 系列交换机

Cisco Nexus 9000 系列交换机（见图 1）是中小型数据中心的理想之选，可提供五项主要优势：价格、性能、端口密度、可编程性和能效。

图 1. Cisco Nexus 9000 系列交换机产品

Cisco Nexus 9000 系列 交换机采用商用增强型交换机设计方法，可实现成本效益。Cisco Nexus 9000 系列交换机的强大功能源自于思科自主开发的芯片及商用芯片专用集成电路 (ASIC) Trident II (T2)。T2 ASIC 还可以提升能效。此外，Cisco Nexus 9000 系列交换机在 10 GB 和 40 GB 每端口密度价格方面领先于市场。Cisco Nexus 9000 系列交换机采用经济高效的设计方法，并且具有丰富的功能集，这使得它非常适合用于商业数据中心。

Cisco Nexus 9000 系列交换机的许可方式得到极大的简化。在撰写本文时，已经提供的许可证有两种：企业服务包许可证用于启用动态路由协议和 VXLAN 支持；思科数据中心网络管理器 (DCNM) 许可证用于为整个数据中心网络提供单一平台 GUI 管理工具。今后随着新功能的推出，可能会提供其他许可证。

Cisco Nexus 9000 系列交换机提供强大的可编程功能，可支持采用 Cisco NX-OS API (NX-API)、Python、Chef 和 Puppet 等工具的新兴网络模型（包括自动化以及开发和运营 [DevOps] 模型）。

对于中小型商业客户，Cisco Nexus 9000 系列交换机产品是 1 GB 到 10 GB 迁移和 10 GB 到 40 GB 迁移的最佳平台，并且是替代数据中心内过时的 Cisco Catalyst® 交换机的理想产品。Cisco Nexus 9000 系列交换机可轻松地与现有网络集成。本白皮书介绍了两台 Cisco Nexus 9000 系列交换机这种小型设计，并且提供了随着数据中心的发展横向扩展数据中心的路径，重点介绍了接入和汇聚设计以及主干-枝叶设计。

关于 Cisco Nexus 9000 系列交换机

Cisco Nexus 9000 系列包括较大的 Cisco Nexus 9500 系列模块化交换机和较小的 Cisco Nexus 9300 系列固定配置交换机。本白皮书后面部分深入讨论了产品配置。

思科为 Cisco Nexus 9000 系列交换机提供了两种操作模式。客户可以使用 Cisco NX-OS 软件在标准的 Cisco Nexus 交换机环境中部署 Cisco Nexus 9000 系列。或者，客户可以使用思科以应用为中心的基础设施 (ACI)，硬件基础设施可随时使用 ACI，以充分利用一种自动化、基于策略的系统管理方法。

除了传统的 Cisco NX-OS 功能（如思科虚拟 PortChannel [vPC]、加电自动调配 [POAP] 和 Nexus 2000 系列交换矩阵扩展器支持）外，Cisco Nexus 9000 系列交换机上运行的单映像 Cisco NX-OS 推出了多项重要的新功能：

- 智能的 Cisco NX - API 为管理员提供了在 HTTP 和/或 HTTPS 上通过远程过程调用（JSON 或 XML）来管理交换机的方法，而非直接访问 Cisco NX-OS 命令行。
- Linux Shell 访问使交换机可以通过 Linux Shell 脚本进行配置，有助于实现多个交换机配置的自动化，以及确保多个交换机之间的一致性。
- 通过冷修补和热修补方法保持持续运行，冷修补和热修补在常规的维护版本之间或在最终维护版本与维护终止版本之间以不具中断性的方式（对于热补丁而言）提供补丁。
- 硬件中以全线速进行的虚拟可扩展局域网 (VXLAN) 桥接和路由可促进并加快虚拟与物理服务器之间的通信。VXLAN 提供与 VLAN 相同的第 2 层以太网服务，但是具有更高的灵活性且大规模提供这些服务。

有关升级的更多信息，请参阅 Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide（Cisco Nexus 9000 系列 NX-OS 软件升级和降级指南）。

Cisco Nexus 9000 系列交换机支持 OpenStack Networking（也称为 Neutron）的插件。使用该插件，您可以构建基础设施即服务 (IaaS) 网络和部署云网络。使用 OpenStack，您可以构建按需、自助服务、多租户的计算基础设施。但是，在虚拟和物理基础设施中实施 OpenStack VLAN 网络模型可能很困难。

OpenStack Networking 可扩展架构支持插件直接配置网络。但是，当您选择某个网络插件时，将只配置该插件的目标技术。当您在 VLAN 的多台主机上运行 OpenStack 集群时，典型的插件将配置虚拟网络基础设施或物理网络，而非同时配置两者。

Cisco Nexus 插件通过支持同时配置物理和虚拟网络基础设施来解决此难题。Cisco Nexus 插件接受 OpenStack Networking API 调用，并使用网络配置协议 (NETCONF) 来配置 Cisco Nexus 设备以及 Open vSwitch (OVS)，后者在虚拟机监控程序上运行。

Cisco Nexus 插件在物理和虚拟网络上配置 VLAN。它还分配稀缺的 VLAN ID，方法是在不再需要 VLAN ID 时取消调配它，然后在可能的情况下将其重新分配给新租户。系统将配置 VLAN，以便在属于同一租户网络的不同虚拟化（计算）主机上运行的虚拟机通过物理网络透明地进行通信。此外，系统对从计算主机到物理网络的连接进行中继，以便只允许流量来自虚拟交换机在主机上配置的 VLAN。

有关更多信息，请参阅 Cisco OpenStack。

本白皮书重点介绍基本设计、集成的各项功能，例如 vPC、VXLAN、接入层设备连接和第 4-7 层服务插入。如需了解 Cisco Nexus 9000 系列交换机上的 Cisco NX-OS 的高级可编程功能，请参阅本文档的“附录 A：自动化和可编程性”。其他功能不属于本白皮书的讨论范围。

思科 ACI 就绪性

思科 ACI 是什么？

思科以应用为中心的基础设施 (ACI) 的网络未来涉及提供以支持快速进行应用变更的方式部署、监控和管理的网络。ACI 通过降低复杂性并采用可自动调配和管理资源的通用策略框架来实现这一目标。

思科 ACI 旨在解决以下业务问题：因主要专注于技术网络调配和变更管理问题而导致应用部署缓慢，解决方法是支持快速部署应用以满足不断变化的业务需求。思科 ACI 提供了一种集成的方法：提供以应用为中心的端到端端到端可视性（从软件重叠一直到物理交换基础设施），同时加快并优化第 4-7 层服务插入，以构建一个为网络提供应用语言的系统。

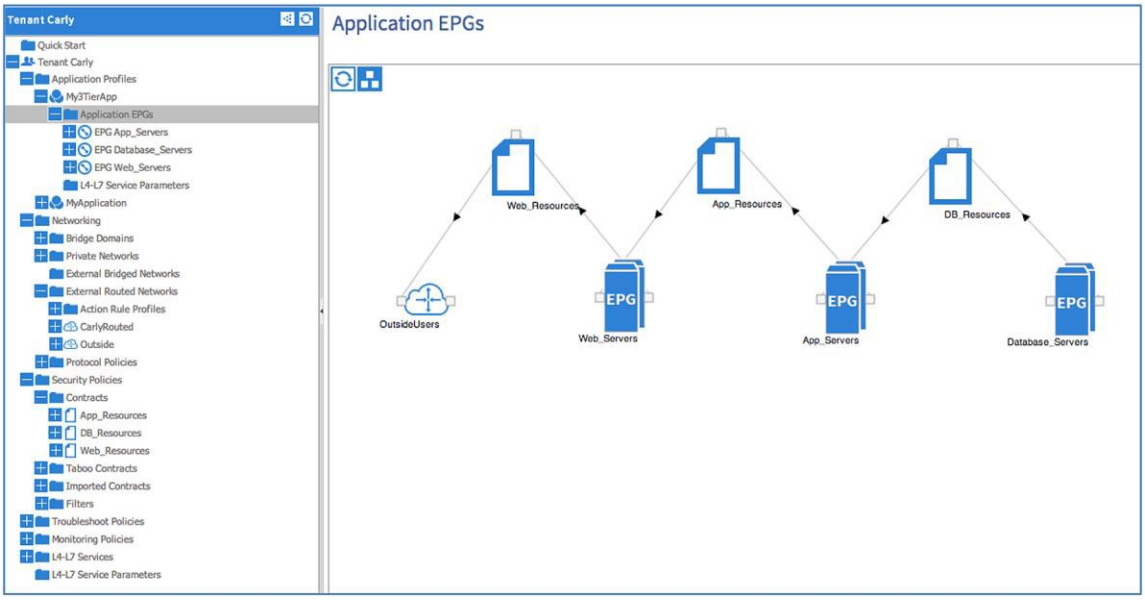
思科 ACI 通过允许根据业务层应用需求使网络自动化和配置网络，来提供自动化、可编程性和集中调配功能。思科 ACI 可在网络和第 4-7 层基础设施中更快地统一部署应用，并在应用层提供可视性和管理能力。使用先进的遥感勘测功能可查看网络运行状况，简化的两天运营也为应用本身的故障排除创造了机会。

思科 ACI 多样化、开放式的生态系统可插入到任何上层的管理或协调系统，吸引了众多的开发者。利用思科和第三方的第 4-7 层虚拟和物理服务设备的集成和自动化功能，您可以使用单个工具管理整个应用环境。

借助思科 ACI 模式，客户可以采用策略的形式根据应用需求部署网路，无需改变当前网络限制的复杂性。此外，思科 ACI 可确保安全性和性能，同时保持全面了解虚拟和物理资源的应用状况。

图 2 显示了如何从思科 ACI GUI 界面为三层应用定义网络通信。按照应用的需求定义网络，通过在应用配置文件内定义一组策略（或合同）标出允许谁与谁通信以及允许它们谈论什么，而不是在多台交换机、路由器和设备上配置一行行的命令行界面 (CLI) 代码。

图 2. 三层应用策略示例



将 Cisco Nexus 9000 NX-OS 模式转换为 ACI 模式

本白皮书重点介绍 NX-OS（单机）模式下的 Cisco Nexus 9000 系列交换机。不过，Cisco Nexus 9000 硬件可支持思科 ACI。Cisco Nexus 9300 交换机和许多 Cisco Nexus 9500 线卡可转换为 ACI 模式。

Cisco Nexus 9000 系列交换机是思科 ACI 架构的基础，并由其提供网络交换矩阵。在 ACI 模式下运行的 Cisco Nexus 9000 交换机使用新的操作系统。这些交换机与名为思科应用策略基础设施控制器 (APIC) 的集中控制器及其开放式 API 结合使用。思科 APIC 可统一对思科 ACI 交换矩阵进行自动化操作、遥感勘测和管理，支持对数据中心采取应用策略模型方法。

在 Cisco Nexus 9000 交换机上从单机 NX-OS 模式转换为 ACI 模式不属于本白皮书的讨论范围。有关 Cisco Nexus 9000 系列交换机的 ACI 模式的更多信息，请参阅思科 ACI 主页。

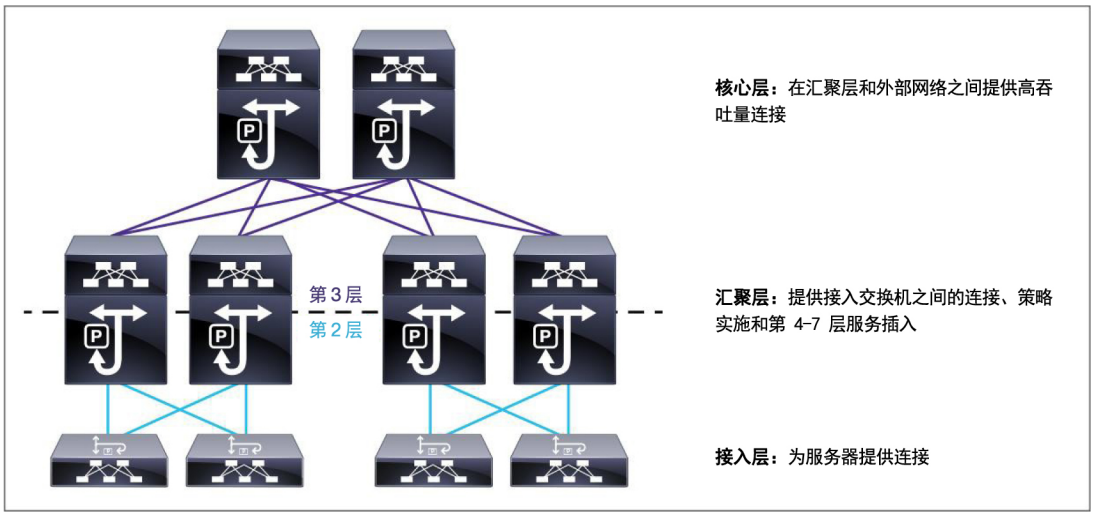
数据中心设计演进

Cisco Nexus 9000 系列交换机可用于中型商业数据中心的多种潜在设计中。Cisco Nexus 9000 系列交换机既可以用作行尾式或架顶式接入层交换机，也可以作为汇聚或核心交换机部署在传统的两层或三层分层网络设计或现代的枝叶-主干架构中。本白皮书讨论了接入和汇聚设计以及枝叶-主干设计。

传统数据中心设计

传统的数据中心采用包含核心、汇聚层和接入层的三层架构构建，或者采用汇聚层和核心层合并在一层的两层紧缩核心构建，如图 3 所示。此架构可适应北-南流量模式，在此模式中，客户端数据来自广域网或互联网，将由数据中心的服务器处理，然后重新从数据中心推出。此模式常用于网络服务等应用，在网络服务中，大多数通信在外部客户端与内部服务器之间进行。南北流量模式允许硬件过载，因为大多数流量通过带宽较低的广域网或互联网瓶颈流入和流出。

图 3. 传统的三层设计



中型商业数据中心最常用的是紧缩两层设计，其中有两项主要的设计决定：

- 第 2 层/第 3 层边界位于汇聚层。
- 第 3 层一直到接入层（路由接入）。

在做出有关第 2 层和第 3 层边界的决定时使用的因素与设计一起讨论，但是每种设计的一些主要考虑事项如表 1 所示：

表 1. 每种设计的主要考虑事项

考虑事项	位于核心层的第 3 层	位于接入层的第 3 层
多路径	每个 VLAN 一个活动路径，因为接入与核心交换机之间采用生成树模式	通过动态路由协议在接入与核心交换机之间进行等价多路径分流
STP	第 2 层链路更多，因此需要阻止的环路和链路更多	没有 STP 在接入层的北向运行
第 2 层可达性	针对工作负载移动性和集群应用提供更高的第 2 层可达性	第 2 层邻接关系限于连接到同一接入层交换机的设备
收敛时间	生成树模式的收敛速度通常比动态路由协议慢	动态路由协议的收敛速度通常比 STP 快

生成树支持

Cisco Nexus 9000 系列支持两种生成树模式：增强型快速每 VLAN 生成树 (PVST+)（这是默认模式）和 MST（多生成树）。

快速 PVST+ 协议是按 VLAN 实施的 IEEE 802.1w 标准，即快速生成树协议 (RSTP)。快速 PVST+ 与 IEEE 802.1Q VLAN 标准互操作。其中 IEEE 802.1Q VLAN 标准要求为所有 VLAN 分配了一个 STP 实例，而不是对每个 VLAN 都分配。默认情况下，快速 PVST+ 在设备上的默认 VLAN (VLAN1) 及新创建的所有 VLAN 上已启用。快速 PVST+ 与运行传统 IEEE 802.1D STP 的设备互操作。RSTP 是对原始 STP 标准 802.1D 的改进，它允许更快速的收敛。

MST 将多个 VLAN 映射到一个生成树实例，每个实例具有独立于其他实例的生成树拓扑。此架构为数据流量提供多条转发路径、支持负载平衡，并可减少支持大量 VLAN 所需的 STP 实例数量。MST 会提高网络的容错能力，因为某个实例中的故障不会影响其他实例。MST 模式通过显式握手提供快速收敛，因为每个 MST 实例都采用 IEEE 802.1w 标准。MST 模式可改进生成树操作，并保持向后兼容原始的 802.1D 生成树和增强型快速每 VLAN 生成树（快速 PVST+）协议。

商业紧缩设计

下面的图 4、5 和 6 描绘了常见于商业数据中心的两层设计，其中第 3 层位于汇聚层，第 2 层从接入层一直向上到汇聚层。有些客户可能不需要完整的两层设计，通常部署一对交换机作为紧缩数据中心架构。

图 4. 传统的一层紧缩设计

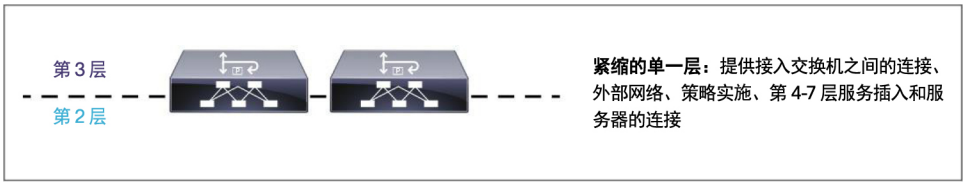


图 5. 传统的两层小型接入-汇聚设计

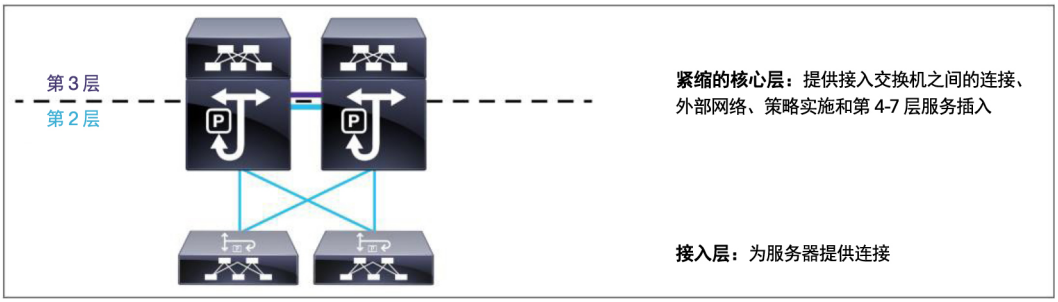
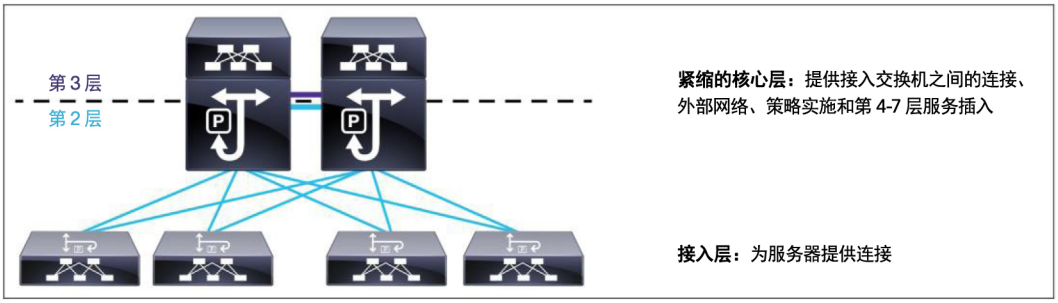
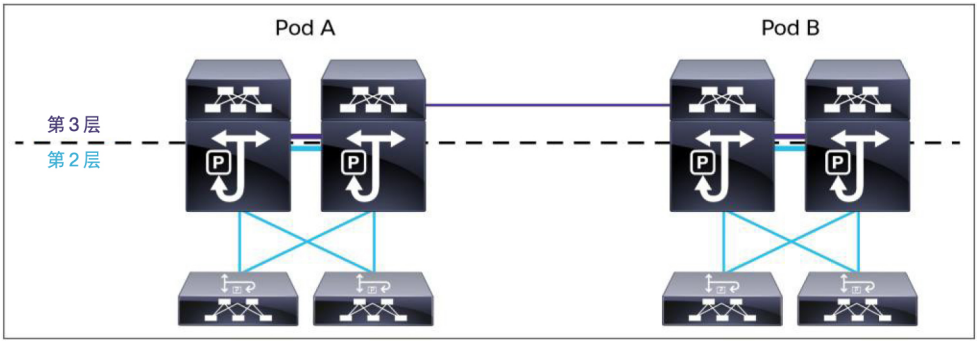


图 6. 传统的两层中型接入-汇聚设计



客户还可以通过 Pod 之间的第 3 层连接将小型紧缩设计复制到其他机架或建筑（图 7）。

图 7. 第 2 层接入、Pod 之间的第 3 层连接

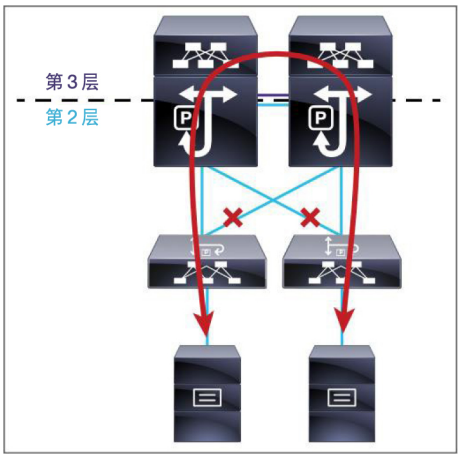


第 2 层与第 3 层影响比较

数据中心流量模式正在不断变化。现在，更多的流量在服务器之间通过接入层按东-西方向流动，因为服务器彼此之间需要通信和使用数据中心的服务。这一转变主要由应用设计的演进推动。许多现代应用需要在数据中心与彼此通信。推动这种转变的应用包括大数据通常采用的分布式处理设计（例如 Hadoop）、实时的虚拟机或工作负载迁移（例如 VMware vMotion）、服务器群集技术（例如 Microsoft 群集服务）和多层应用。过载的硬件现在不足以应对 10 GB 到 10 GB 的东-西通信。此外，东-西流量通常采用次优路径被迫上行通过核心层或汇聚层。

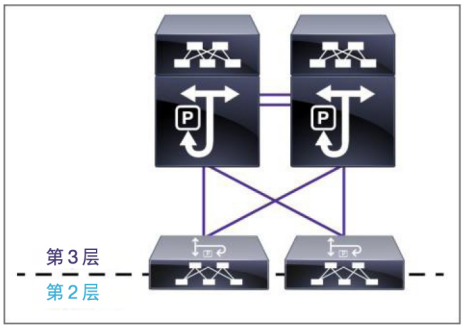
生成树是传统的三层数据中心设计的另一种障碍。需要使用生成树阻止环路在以太网网络中泛滥，以便帧不会被无止境地转发。阻止环路意味着阻止链路，只保留一个活动路径（每个 VLAN）。阻止链路会严重影响可用带宽和过载。这种情况还会迫使流量采用次优路径，因为生成树会阻止更理想的路径。

图 8. 不同 Pod 中的服务器之间因生成树阻止链路而采用的次优路径



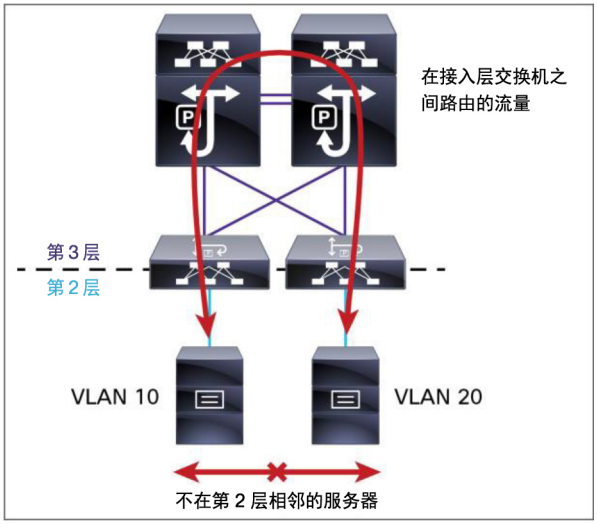
解决这些问题可能包括升级硬件以支持 40 GB 或 100 GB 接口，将链路绑定到思科端口通道以显示为生成树的一条逻辑链路，或将第 2 层-第 3 层边界向下移至接入层以限制生成树的可达性。在两层之间使用动态路由协议使所有链路成为活动链路，并且可以快速进行重新收敛和等价多路径分流 (ECMP)。

图 9. 两层路由接入层设计



在传统以太网网络中，将第 3 层路由移至接入层时的权衡限制了第 2 层可达性。虚拟机工作负载移动性等应用和某些集群软件要求源服务器与目标服务器之间在第 2 层邻接。在接入层路由时，只有连接到同一接入交换机且相同 VLAN 向下中继的服务器在第 2 层邻接。但是，由于以太网的广播性质和生成树重新收敛事件，这种在整个数据中心生成 VLAN 以提高可达性的替代方法是有问题的。

图 10. 路由接入层限制了第 2 层可达性

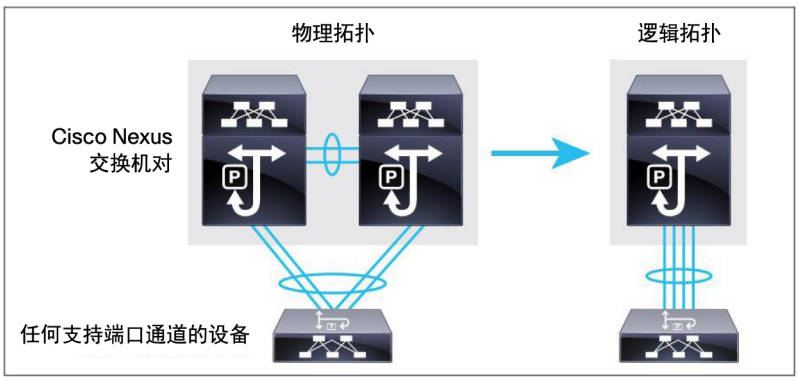


思科第 2 层设计演进：虚拟 PortChannel

在过去几年，许多客户寻找各种方法来跨越生成树的限制。随着思科虚拟 PortChannel (vPC) 的出现，通往基于 Cisco Nexus 解决方案的现代数据中心之路的第一步在 2008 年迈出。vPC 使设备可以使用单个思科 PortChannel 逻辑接口连接到两台不同的 Cisco Nexus 物理交换机。

在思科 vPC 之前，思科 PortChannel 通常必须在单个物理交换机上终止。思科 vPC 为设备提供主用 - 主用转发路径。由于两台 Cisco Nexus 交换机之间的特殊对等关系，生成树看不到任何环路，使所有链路都处于活动状态。对于连接的设备，连接显示为正常的思科 PortChannel 接口，不需要特殊配置。行业标准术语称为“多机箱 EtherChannel”；Cisco Nexus 实施称为“vPC”。

图 11. vPC 物理拓扑与逻辑拓扑比较



在生成树以太网网络上部署的思科 vPC 是抑制被阻止链路数量非常有效的方式，因而可提高可用的带宽。Cisco Nexus 9000 交换机上的思科 vPC 解决方案非常适合商业客户以及对当前带宽、过载和第 2 层可达性要求不满意的客户。

使用图 12 中的 vPC 描绘了中小型传统商业拓扑的两个示例，这些设计使第 2 层-第 3 层边界位于汇聚层，以实现更大的第 2 层可达性，但是所有链路都处于活动状态，因为生成树看不见任何要阻止的链路。本白皮书稍后部分将讲述有关 Nexus 交换机之间的特殊 vPC 对等关系的详细信息。

图 12. 思科 vPC 的传统一层紧缩设计

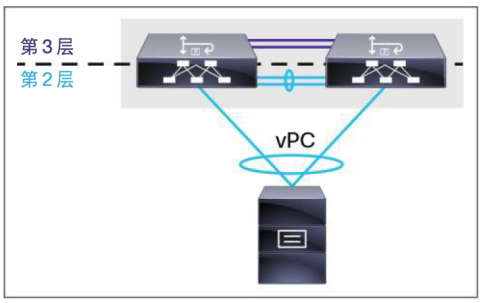
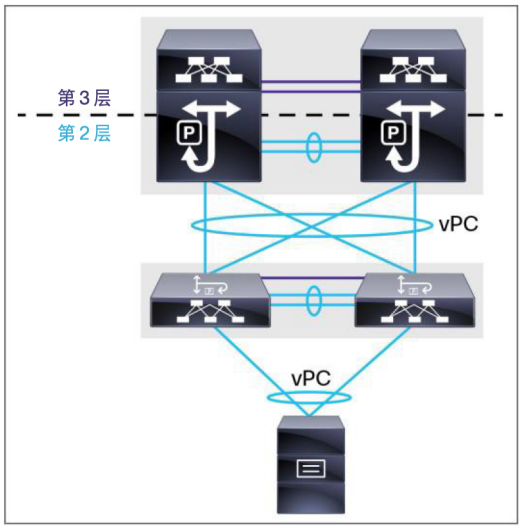


图 13. 思科 vPC 的传统两层设计

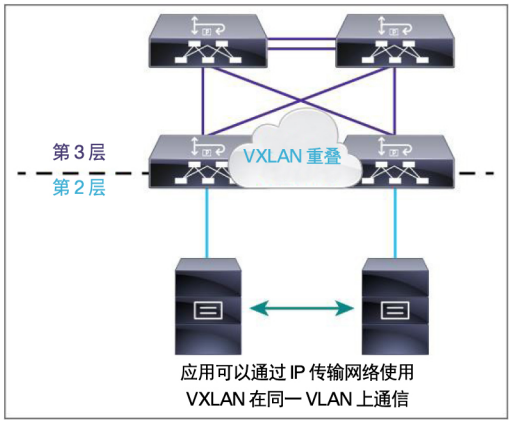


虚拟重叠

如果客户采用两层或三层设计，并且寻求路由至接入层但仍在服务器之间保持第 2 层可达性，则客户可以通过实施虚拟重叠交换矩阵迈出数据中心演进的下一步。在 Cisco Nexus 9000 交换矩阵设计中，在交换机之间配置动态路由（一直到接入层），因此所有链路都处于活动状态。这样做可以消除交换矩阵上对生成树的需要，并通过动态路由协议启用 ECMP。

名为“虚拟可扩展局域网 (VXLAN)”的虚拟重叠交换矩阵可以用于通过第 3 层交互矩阵，为 Cisco Nexus 9000 设计中的服务器和需要第 2 层可达性的其他设备提供第 2 层邻接关系。将 VXLAN 和动态路由协议相结合可提供智能的第 3 层路由协议的优势，同时还可以为虚拟机工作负载移动性和集群等应用提供涵盖所有接入交换机的第 2 层可达性。

图 14. 通过底层 IP 传输网络进行的启用 VXLAN 的第 2 层通信



三层设计中的生成树局限和现代应用的需求正在推动网络设计向主干-枝叶或接入和汇聚架构转变。两层和三层设计仍然是有效且流行的架构；主干-枝叶架构提供另一个轻松集成的选项。

主干-枝叶数据中心设计

主干-枝叶拓扑基于 Clos 网络架构。Clos 一词源自贝尔实验室的 Charles Clos，他在 1953 年发表了一篇论文，其中介绍了一种通过多路径、无阻塞、多级的网络拓扑交换电话呼叫的数学理论。

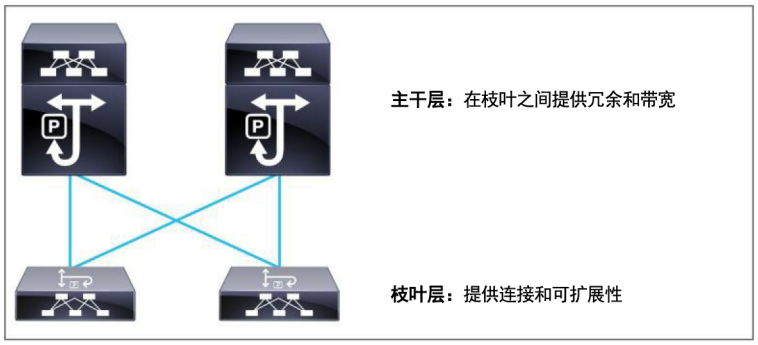
现在，Clos 的原始设计理念应用于现代的主干-枝叶拓扑。主干-枝叶架构通常部署为两层：主干（例如汇聚层）和枝叶（例如接入层）。主干-枝叶拓扑提供高带宽、低延迟、无阻塞的服务器到服务器连接。

枝叶（汇聚）交换机使设备可以访问交换矩阵（由主干和枝叶交换机组成的网络），通常部署在机架顶部。通常，设备连接到枝叶交换机。设备可以包括服务器、第 4-7 层服务（防火墙和负载平衡器）以及广域网或互联网路由器。枝叶交换机不连接到其他枝叶交换机（除非在单机 NX - OS 模式下运行 vPC）。但是，每个枝叶应连接到全网状网络中的每个主干。枝叶上的某些端口用于终端设备（通常为 10 GB），某些端口用于主干连接（通常为 40 GB）。

主干（汇聚）交换机用于连接到所有枝叶交换机，通常部署在行尾或中间。主干交换机不连接到其他主干交换机。主干交换机用作枝叶交换机的主干互联。通常，主干仅连接到枝叶，但是在将 Cisco Nexus 9000 交换机与现有环境集成时，可以接受将其他交换机、服务或设备连接到主干。

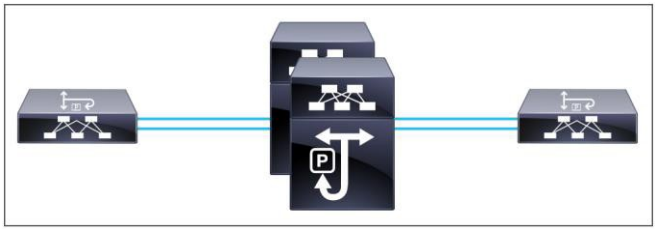
连接到交换矩阵的所有设备距离所有其他设备的跳数相同。这使服务器之间的延迟时间可预测并且提供高带宽。图 15 描绘了简单的两层设计。

图 15. 两层设计和连接



思考主干-枝叶架构的另一种方法是将主干看作中央骨干，所有枝叶像星星一样从主干分叉出去。图 16 描绘了这种逻辑表示，它在备用可视映射配置中使用相同的组件。

图 16. 两层设计的逻辑表示



采用 Cisco Nexus 9000 系列交换机，中小型商业客户可以先从使用几台交换机开始，实施“随增长，随投资”模式。在需要更多接入端口时，可以添加更多枝叶（接入交换机）。在需要更多带宽时，可以添加更多主干（汇聚交换机）。Cisco Nexus 9000 交换机非常适合传统设计、主干-枝叶或现有拓扑的任意组合。

重叠设计

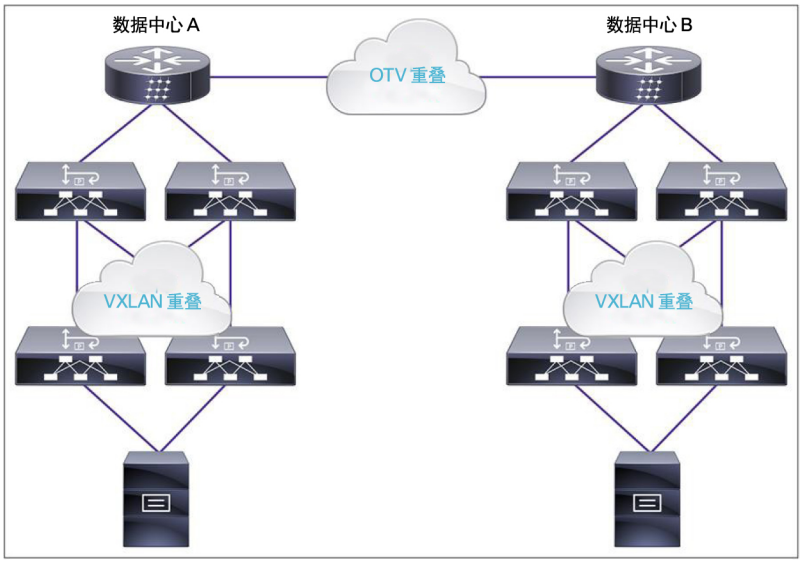
虚拟网络重叠将物理网络基础设施划分成多个可以单独编程和管理的逻辑隔离网络，以提供最佳的网络需求。

中小型商业客户可能要求在数据中心之间、在单个数据中心的不同 Pod 之间以及在整个第 3 层网络边界中具有移动性。虚拟网络重叠使移动性和第 2 层可达性成为可能。

思科在开发多个重叠网络上发挥了作用，每个重叠网络通过提供创新的解决方案解决不同的问题。例如，思科重叠传输虚拟化 (OTV) 功能使用“MAC-in-IP”封装方式在第 3 层思科数据中心互联 (DCI) 网络上提供跨数据中心的移动性。

图 17 显示了正在使用的两个重叠网络：思科 ASR 1000 路由器上的思科 OTV（用于数据中心之间的连接），以及数据中心内的 VXLAN。两者提供第 2 层可达性和扩展。Cisco Nexus 7000 系列交换机上也提供思科 OTV 功能。

图 17. 为应用提供动态可达性的虚拟重叠网络

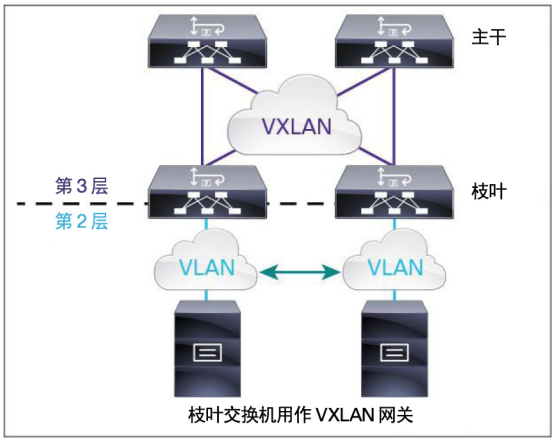


有关重叠的更多一般信息，请参阅 Data Center Overlay Technologies white paper（数据中心重叠技术白皮书）。有关思科 OTV 的更多信息，请参阅思科 OTV 网页。

现在，Cisco Nexus 9000 系列交换机上具有 IETF 建议的 VXLAN 重叠功能，该功能跨数据中心的 IP 传输网络提供第 2 层连接扩展，并且在 VXLAN 与非 VXLAN 基础设施之间轻松集成。VXLAN 通过一个共享的通用物理基础设施启用可扩展的虚拟化和多租户数据中心设计。

除了在这些交换机上发起和终止的简单重叠外，Cisco Nexus 9000 交换机还可以用作基于硬件的 VXLAN 网关。VXLAN 越来越普遍地用于虚拟机监控程序中的虚拟网络，适用于虚拟机间的通信，而非仅限于交换机间的通信。但是，许多设备没有能力支持 VXLAN，例如传统的虚拟机监控程序、物理服务器以及服务设备，如防火墙、负载平衡器和存储设备。这些设备需要继续驻留在传统的 VLAN 网段。VLAN 网段中的虚拟机有时需要访问由传统 VLAN 网段中的设备提供的服务，这种情况并不少见。用作 VXLAN 网关的 Cisco Nexus 9000 交换机可以提供必要的转换。

图 18. 将 VLAN 转换为 VXLAN 的 Cisco Nexus 9000 枝叶交换机



现在，必须由外部设备提供数据中心互联 (DCI)，例如思科 OTV。在 VXLAN 的下一阶段，Cisco Nexus 9000 交换机支持边界网关协议 (BGP) 以太网 VPN (EVPN)。EVPN 是基于 BGP 控制平面的下一代第 2 层 VPN 解决方案，它可以用作数据中心互联解决方案，在核心或运营商 IP 网络中发布 MAC 地址可达性信息。

有关更多信息，请参阅“IETF BGP MPLS Based Ethernet VPN”(draft)（基于 BGP MPLS 的以太网 VPN IETF 草案）。

用于枝叶（或接入）交换机之间的第 2 层扩展的基本 VXLAN 桥接是本白皮书中的特色设计，后面部分将更深入进行讨论。

其他 Cisco Nexus 9000 功能支持

虽然已讨论许多新功能和重要功能，但是有必要重点介绍 Cisco Nexus 9000 系列交换机提供的其他功能支持，例如服务质量 (QoS)、组播以及简单网络管理协议 (SNMP) 和支持的 MIB。

服务质量

新应用和不断发展的协议正在改变现代数据中心的 QoS 要求。高频率交易大厅应用对延迟非常敏感，而高性能计算的特征通常是突发、多对一的东-西流量。任何数据中心内的存储、语音和视频等应用也需要特殊且不同的处理。

像 Cisco Nexus 系列的其他成员一样，Cisco Nexus 9000 系列交换机通过思科模块化 QoS CLI (MQC) 支持 QoS 配置，这涉及根据协议或数据包报头标记等信息使用类映射来识别流量，定义如何通过策略映射来处理不同的类，可能采用的方法是标记数据包、排队或调度，最后使用服务策略命令将策略映射应用于接口或整个系统。QoS 在默认情况下处于启用状态，且不需要许可证。

与 Cisco IOS® 不同，Cisco Nexus 9000 交换机上的 Cisco NX-OS 使用三种不同的策略映射类型，具体取决于您尝试实施的 QoS 功能。Cisco NX-OS QoS 的三种类型及其主要用途包括：

- **QoS 类型：**
  - 分类
  - 标记
  - 策略管制

- **排队类型：**
  - 缓冲
  - 排队
  - 调度
- **网络-QoS 类型：**
  - 系统范围的设置
  - 堵塞控制
  - 暂停行为

网络-QoS 类型的策略映射仅应用于系统范围内，而 QoS 类型和排队类型可以各自同时应用于单个接口，一种类型应用于每个入口和出口，每个接口共四个 QoS 策略（如果需要）。

在 Cisco Nexus 9500 交换机上，可以根据报头地址字段、802.1p CoS（服务类别）、IP 优先级、差分服务代码点 (DSCP) 值等属性对入口流量进行分类，也可以根据访问控制列表 (ACL) 匹配入口流量。在分类后，流量可分配给四个 QoS 组之一。QoS 组用作流量类的内部标识，该标识在数据包经过系统时用于后续的 QoS 流程。在入口，Cisco Nexus 9500 交换机还可以重新标记 CoS、IP 优先级和 DSCP，以及执行基于类的策略管制。

在出口，Cisco Nexus 9500 交换机使用简单的排队架构，并且不像其他 Cisco Nexus 平台那样在入口线卡端口上使用虚拟输出队列 (VoQ)。如果出口端口拥塞，数据包直接在出口线卡的缓冲区中排队，大大简化系统缓冲区管理和排队实施。Cisco Nexus 9500 交换机最多可在出口上支持六个流量类（四个通过 QoS 组 ID 标识的用户定义类、一个 CPU 控制流量类和一个 SPAN 流量类）。每个用户定义类的每个出口端口可包含一个单播队列和一个组播队列。网络转发引擎 (NFE)（Trident II ASIC [专用集成电路]）上的 12 MB 缓冲区在本地端口之间共享。缓冲区的资源由入口和出口流量动态共享。交换机软件设置了一项机制，用于测量和限制各出口端口的缓冲使用情况。这样可确保任何一个端口消耗的缓冲区内存空间均不会超出平均值，继而避免其他端口出现缓冲空间匮乏情况。

此外，在出口，Cisco Nexus 9500 交换机最多可提供三个基于优先级的流量控制无丢弃队列、三个严格优先级队列，并且能够启用加权随机早期探测 (WRED) 或显式拥塞通知 (ECN)，而非默认的尾部丢弃队列管理。

思科 ACI 就绪枝叶线卡的每个思科 ACI 枝叶引擎 (ALE) 中还具有一个额外的 40MB 缓冲区。该缓冲区有 10MB 分配给交换矩阵绑定的流量。剩余 30MB 则分配给来自交换矩阵模块的出口流量和从高速入口端口发送到低速出口端口的本地交换流量。

这 30MB 缓冲空间用于单播流量的扩展输出列队。NFE 通过带外流量控制 (OOBFC) 信令通道向思科 ALE 传达单播队列状态。当出口队列超出配置的阈值时，NFE 会发送 OOBFC 信号以指示思科 ALE 停止转发此队列的流量，开始在其自身的缓冲区中排列数据包。接到该信号后，思科 ALE 开始在给定的出口端口上为此流量类建立扩展输出队列。当出口队列长度减少到配置的重新启动阈值后，NFE 将发送另一个 OOBFC 信号，以指示思科 ALE 恢复传输这个特定队列的流量。

- 有关通过 ASIC 进行的单播和组播数据包转发的更多详情，请参阅白皮书 Cisco Nexus 9500 Series Switches Architecture（Cisco Nexus 9500 系列交换机架构）。

如需了解混合局域网和存储环境中的其他 QoS 注意事项，请参阅“Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide, Release 6.0”（Cisco Nexus 9000 系列 NX-OS 服务质量配置指南 6.0 版）

组播

在启用组播路由的情况下，Cisco Nexus 9500 平台以最多 8000 个组播路由的规模低延迟地提供高性能、线速的第 2 层和第 3 层组播吞吐量。Cisco Nexus 9500 平台通过为第 2 层和第 3 层组播执行基于 IP 的查找来优化组播查找和复制，以避免出现组播 IP 至 MAC 编码中常见的别名问题。

Nexus 9500 平台支持互联网组管理协议 (IGMP) 版本 1、2 和 3，以及协议无关组播 (PIM) 稀疏模式、任意播交汇点和组播源发现协议 (MSDP)。

SNMP 和支持的 MIB

简单网络管理协议 (SNMP) 提供标准框架和语言来管理网络上的设备，包括 Cisco Nexus 9000 系列交换机。SNMP 管理器使用 SNMP 控制和监控网络设备的活动。SNMP 代理在受管设备中运行，并将数据报告给管理系统。Cisco Nexus 9000 系列交换机上的代理必须配置为与管理器通信。MIB 是 SNMP 代理的受管对象集合。Cisco Nexus 9000 系列交换机支持 SNMP v1、v2c 和 v3。Cisco Nexus 9000 系列交换机还可以支持基于 IPv6 的 SNMP。

SNMP 会生成关于 Cisco Nexus 9000 系列交换机的通知并发送给管理器，例如在邻近路由器丢失时通知管理器。陷阱通知从 Cisco Nexus 9000 交换机上的代理发送给管理器，管理器未确认消息。用于告知的通知由管理器确认。表 2 提供了默认情况下启用的 SNMP 陷阱。

表 2. Cisco Nexus 9000 系列交换机上默认情况下启用的 SNMP 陷阱

陷阱类型	说明
generic	: coldStart
generic	: warmStart
entity	: entity_mib_change
entity	: entity_module_status_change
entity	: entity_power_status_change
entity	: entity_module_inserted
entity	: entity_moudle_removed
entity	: entity_unrecognised_module
entity	: entity_fan_status_change
entity	: entity_power_out_change
link	: linkDown
link	: linkup
link	: extended-linkDown
link	: extended-linkUp
link	: cieLinkDown
link	: cieLinkUp
link	: delayed-link-state-change

陷阱类型	说明
rf	: redundancy_framework
license	: notify-license-expiry
license	: notify-no-license-for-feature
license	: notify-licensefile-missing
license	: notify-license-expirty-warning
upgrade	: UpgradeOpNotifyOnCompletion
upgrade	: UpgradeJobStatusNotify
rmon	: risingAlarm
rmon	: fallingAlarm
rmon	: hcRisingAlarm
rmon	: hcFallingAlarm
entity	: entity_sensor

在 Cisco Nexus 9000 交换机上，Cisco NX-OS 支持无状态重新启动，并且也知道虚拟路由和转发 (VRF)。使用 SNMP 不需要许可证。

有关 Cisco Nexus 9000 系列交换机上支持的 MIB 的列表，请参阅此列表。

如需获得配置帮助，请参阅“Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 6.0”（Cisco Nexus 9000 系列 NX-OS 系统管理配置指南 6.0 版）中的 Configuring SNMP（配置 SNMP）部分。

商业拓扑示例

使用 10 和 40 千兆以太网的主干-枝叶或接入-汇聚架构旨在处理数据中心向东-西流量模式的转变，通过在层之间路由来限制生成树的范围，提供无环路、所有链路都处于活动状态的拓扑，执行 ECMP，并可选择使用 VXLAN 为第 2 层可达性提供虚拟重叠。

在部署 Cisco Nexus 9000 交换机时不需要主干-枝叶设计，而且该拓扑可视作接入-汇聚架构，在本白皮书中该拓扑也称为接入-汇聚。

Cisco Nexus 9000 系列交换机产品组合提供一系列可供选择的交换机。设计考虑事项包括期望吞吐量、过载比、预计增长率、服务器流量模式和应用需求等。

此部分概述了 Cisco Nexus 9000 系列交换机产品组合，并介绍了适合中小型商业数据中心的几种设计。此部分还显示了简单的网络拓扑。本白皮书后面部分的商业拓扑示例演示了如何将这些设计选项与现有网络集成。

Cisco Nexus 9500 平台产品系列

Cisco Nexus 9500 平台模块化交换机在商业数据中心中通常部署为主干（汇聚或核心交换机）。图 19 列出了在撰写本文时 Cisco Nexus 9500 机箱在 NX-OS 单机模式下提供的线卡。（仅适用于思科 ACI 的线卡已被移除。）

图 19. Cisco Nexus 9500 线卡类型

模块化：Cisco Nexus 9500 线卡类型

线卡	端口	模式	交换矩阵模块	机箱支持
X9600				
X9636PQ	36 端口 QSFP+	NX-OS	6	N9504、N9508
X9500				
X9564PX	48 端口 1/10G SFP+ 和 4 端口 QSFP+	NX-OS、ACI	3	N9504、N9508、N9516
X9564TX	48 端口 1/10G-T 和 4 端口 QSFP+	NX-OS、ACI	3	N9504、N9508、N9516
X9536PQ	36 端口 QSFP+ (1.5:1)	NX-OS、ACI	3	N9504、N9508、N9516
X9400				
X9464PX	48 端口 1/10G SFP+ 和 4 端口 QSFP+	NX-OS	2	N9504、N9508、N9516
X9464TX	48 端口 1/10G-T 和 4 端口 QSFP+	NX-OS	2	N9504、N9508、N9516
X9432PQ	32 端口 QSFP+	NX-OS	4	N9504、N9508、N9516

注意：如需获得最新的产品信息，请参阅 Cisco Nexus 9500 data sheets（Cisco Nexus 9500 产品手册）。自撰写本文以来，线卡可用性可能已经发生变化。

Cisco Nexus 9300 平台产品系列

Cisco Nexus 9300 平台固定配置交换机通常部署为枝叶（接入交换机）。某些 Cisco Nexus 9300 交换机通过为额外的端口提供上行链路模块插槽成为半模块化交换机。下图列出了在撰写本文时提供的支持 NX-OS 单机模式的 Cisco Nexus 9300 机箱。

图 20. Cisco Nexus 9300 系列机箱配置

固定：Cisco Nexus 9300

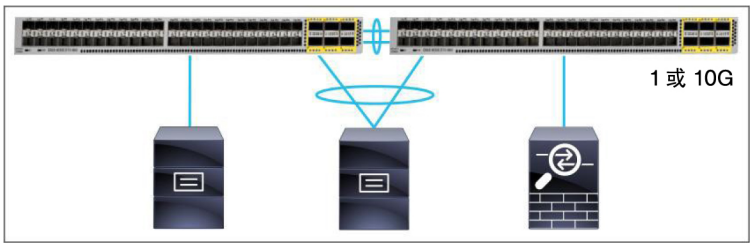
线卡	端口	模式	RU	上行链路模块
N9396PX	48 端口 1/10G SFP+ 和 12 端口 QSFP+	NX-OS、ACI	2	有
N9396TX	48 端口 1/10G-T 和 12 端口 QSFP+	NX-OS、ACI	2	有
N93128TX	96 端口 1/10G-T 和 8 端口 QSFP+	NX-OS、ACI	3	有
N93128TX2	96 端口 1/10G-T 和 8 端口 QSFP+	NX-OS、ACI	2	无
N93128PX2	96 端口 1/10G SFP+ 和 8 端口 QSFP+	NX-OS、ACI	2	无
N9372PX	48 端口 1/10G SFP+ 和 6 端口 QSFP+	NX-OS、ACI	1	无
N9372TX	48 端口 1/10G-T 和 6 端口 QSFP+	NX-OS、ACI	1	无
N9332PQ	32 端口 QSFP+	NX-OS、ACI	1	无
N9332PQ2	32 端口 QSFP+	NX-OS、ACI	2	有

注意：如需获得最新的产品信息，请参阅 Cisco Nexus 9300 data sheets（Cisco Nexus 9300 产品手册）。自撰写本文以来，交换机可用性可能已经发生变化。

设计 A：两台交换机

小型商业客户可以部署一对 Cisco Nexus 9300 交换机。可以在 Cisco Nexus 9300 交换机上配置 vPC，使连接的设备能够对于每台交换机拥有两个主用、冗余的路径（图 21）。

图 21. 两台交换机的小型企业部署



该拓扑描绘了一对固定的 1 机架单元 (1RU) Cisco Nexus 9372PX 交换机。每台 Cisco Nexus 9372PX 交换机提供 48 端口的 1/10 千兆以太网，具有增强型小型封装热插拔 (SFP+) 收发器和 6 个四 (4) 通道小型封装热插拔 (QSFP+) 40 GB 端口。如果 10 GB 的 SFP+ 上需要双绞线 RJ-45 接头，还可以使用该交换机的 10GBASE-T 版本。此设计在一个 2RU 机箱中总共提供 108 个端口，支持 1 GB、10 GB 和 40 GB 接口。

如果不需要 40 GB 接口，可以使用思科 QSFP 至 SFP 或 SFP+ 适配器 (QSA) 模块这些端口转换为 10 GB 接口。Cisco QSA 模块将 40 GB QSFP 端口转换为 1 GB SFP 或 10 GB SFP+ 端口。客户可以灵活地使用任何 SFP+ 和 SFP 模块或电缆连接到低速端口。这种灵活性使得可以在一段时间后经济高效地过渡到 40 GB。Cisco QSA 模块支持所有 SFP+ 光纤和电缆连接以及多个 1 GB SFP 模块。

图 22. 空的 Cisco QSA 模块（左侧）；已插入 SFP 或 SFP+（右侧）

有关 Cisco QSA 模块的更多信息，请参阅 Cisco QSA data sheet（Cisco QSA 产品手册）。

有关在 10 GB 接口上节省资金以及适用于 10 米以下距离的思科 SFP+ Twinax 直连铜缆的信息，请点击此处。使用 Twinax 电缆（图 23）可在传统的 10 GB 光纤收发器和布线上节省大量资金。

图 23. 带 SFP+ 接头的思科 Twinax 直连铜缆组件

有关所有 10 GB SFP+ 电缆选项的更多信息，请参阅 Cisco 10GBase SFP Modules data sheet（Cisco 10GBase SFP 模块产品手册）。

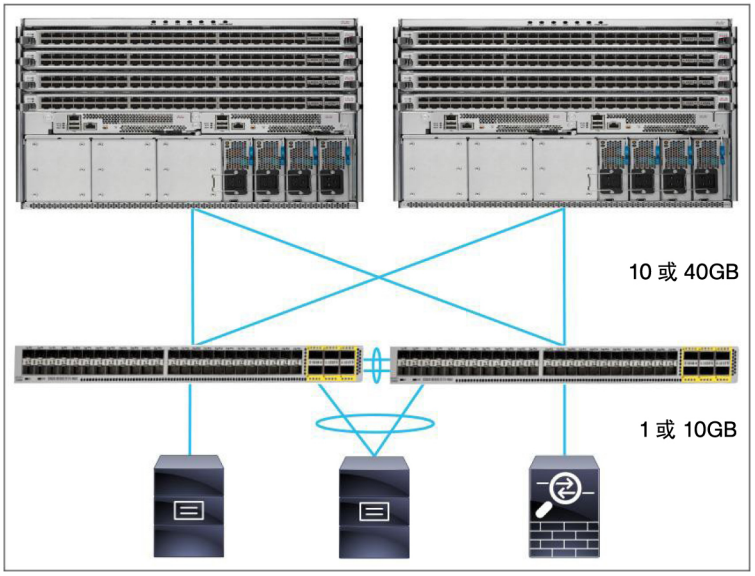
请务必查看 Cisco Transceiver Modules compatibility information（思科收发器模块兼容性信息）网页，了解关于机箱支持的最新信息。

采用两台交换机设计时，小型企业可获得 Cisco Nexus 9000 解决方案的优势，同时利用较小、价格实惠的机箱空间带来的益处。在一段时间后，随着数据中心不断发展，需要更多吞吐量时，客户可以通过添加更多枝叶（接入交换机）来扩展设计，或者可以选择在汇聚（或主干）层中添加 Cisco Nexus 9500 平台，这是下一种重点介绍的拓扑。

设计 B：两台汇聚交换机和两台接入交换机

简单的两主干（汇聚）和两枝叶（接入）设计为需要更多带宽和未来扩展空间的中小型客户提供令人满意的起点，如图 24 所示。

图 24. 适用于中小型企业的两汇聚、两接入商业设计



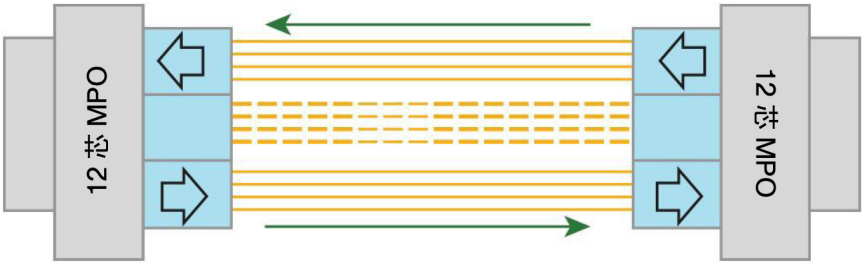
在枝叶（或接入）层，此处显示的拓扑描绘了一对固定的 1RU Cisco Nexus 9372PX 交换机。每台 Cisco Nexus 9372PX 交换机提供 48 端口的 1/10 千兆以太网，具有 SFP+ 收发器和 6 个 QSFP+ 40 GB 端口。如果 10 GB 的 SFP+ 上需要双绞线 RJ-45 接头，还可以使用该交换机的 10GBASE-T 版本。

在主干（或汇聚）层，该拓扑描绘了具有 N9K-X9536PQ 线卡的两个 Cisco Nexus N9K-C9504 机箱。这些线卡各提供 36 个 QSFP+ 40 GB 端口，用于连接到枝叶。在为接入端口添加更多枝叶时，9536PQ 36 端口线卡为未来的增长敞开大门，并且为过渡到 ACI 模式提供方便。

如需获得线卡之间的最新比较信息，请参阅 Cisco Nexus 9000 Series Switches Compare Models tool（Cisco Nexus 9000 系列交换机型号对比工具）。

当您从 10 GB 过渡到 40 GB 时，Cisco QSA 40 GB 至 10 GB 模块也可以用在此设计中。或者，思科提供名为 BiDi 的低成本 40 GB 收发器，使从 10 GB 迁移到 40 GB 变得容易。现有的短距 40 GB 收发器通过一个多芯光纤推接式 (MPO) 接头使用需要 12 条光纤线束的接头。遗憾的是，现有的 10 GB 光纤部署和接线板使用朗讯接头 (LC) 到 LC 多模光纤。如果所有收发器、布线和接线板必须更换，则从 10 GB 升级到 40 GB 光纤可能是一项成本高昂的任务。

图 25. 现有的 40 GB 12 线束光缆和接头



作为替代方案，Cisco 40G QSFP BiDi 收发器（图 25 ）通过提供在带 LC 接头的标准 OM3 或 OM4 多模光纤上传输全双工 40 GB 的能力，来应对光纤基础设施的挑战。Cisco BiDi 收发器可以重复利用现有的 10 GB 光纤布线，而不是部署新的光纤基础设施。现在，Cisco BiDi 光纤收发器以和 10 GB 光纤几乎相同的成本提供经济实惠、简单的 40 GB 升级路径。

图 26. Cisco QSFP BiDi 收发器

图 27. Cisco BiDi 光纤连接和速度

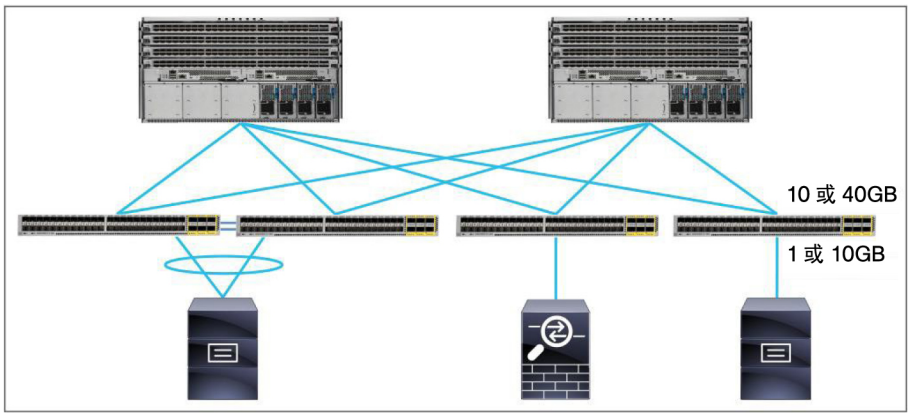
有关 Cisco BiDi 光纤的更多信息，请参阅 Cisco QSFP BiDi Technology white paper（Cisco QSFP BiDi 技术白皮书）。

本白皮书后面部分展示了此设计，并提供了配置示例。

设计 C：两台汇聚交换机和四台接入交换机

随着您的数据中心不断发展以及添加更多服务器，可以通过添加更多枝叶（接入交换机）来扩展 Cisco Nexus 9000 部署，以增加可用的服务器和设备接入端口，如图 28 所示。

图 28. 两汇聚、四接入商业增长设计



在枝叶（或接入）层，该拓扑描绘了四台固定的 1RU Cisco Nexus 9372PX 交换机。每台 Cisco Nexus 9372PX 交换机提供 48 端口的 1/10 千兆以太网，具有 SFP+ 收发器和 6 个 QSFP+ 40 GB 端口。如果 10 GB 的 SFP+ 上需要双绞线 RJ-45 接头，还可以使用该交换机的 10GBASE-T 版本。

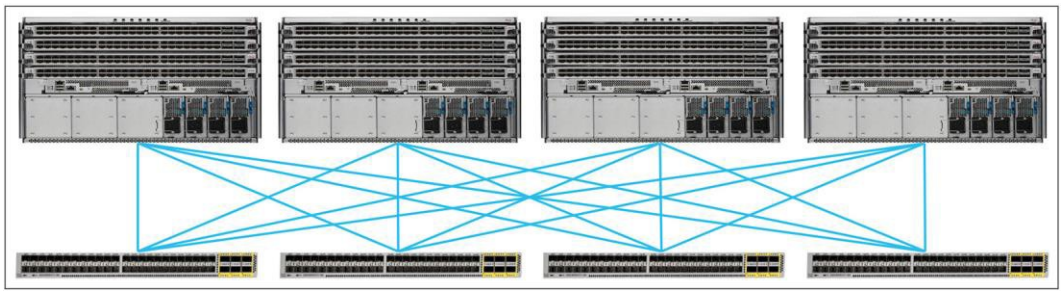
在主干（或汇聚）层，该拓扑描绘了具有 Cisco N9K- X9536PQ 线卡的两个 Cisco Nexus N9K-C9504 机箱。这些线卡各提供 36 个 QSFP+ 40 GB 端口，用于连接到枝叶。在为接入端口添加更多枝叶时，Cisco 9536PQ 36 端口线卡为未来的增长敞开大门。这些线卡还为过渡到 ACI 模式提供方便。

设计 D：四台汇聚交换机和四台接入交换机（采用主干-枝叶架构）

拥有至少四个主干的设计意味着形成真正的主干-枝叶拓扑，主干的功能变成纯粹的主干连接。在此设计中，连接到主干的设备只有枝叶。单个主干的故障对系统的影响微乎其微，只是留下一条可用性较低的路径。所有设备均连接到枝叶。

添加主干会在交换矩阵中提供更多交叉带宽，以及用于平衡流量负载的额外路径。像之前的设计一样，在需要更多接入端口时，可以将更多枝叶添加到拓扑中。随着带宽需求增加，还可以添加更多主干。使用主干-枝叶拓扑可以大规模扩展。

图 29. 四主干、四枝叶的可扩展带宽设计



与现有网络集成

将 Cisco Nexus 9000 系列交换机添加到数据中心并不意味着必须移除或重新配置现有设备。Cisco Nexus 9000 解决方案可轻松地与商业数据中心集成，同时仍然提供该平台的所有优势。

接入层设备连接

服务器、存储设备和第 4-7 层服务设备可以连接到 Cisco Nexus 9500 主干（汇聚）或 Cisco Nexus 9300 枝叶（接入）交换机，或者保留在现有的数据中心交换机不变，具体视您现有的网络而定。

在真正的主干-枝叶拓扑中，所有设备直接连接到枝叶，连接到主干的设备只有枝叶。此拓扑提供可预测的延迟，并确保每台设备距离交换矩阵中任何其他设备的跳数相同。

随着 Cisco Nexus 9300 枝叶的新 Pod 添加到网络中，可以将新服务器连接到接入层的枝叶。其他设备（例如 Cisco Nexus 5000 系列交换机、思科统一计算系统™ (Cisco UCS®) 或刀片服务器接入层设备）可以连接到 Cisco Nexus 9000 系列交换机。

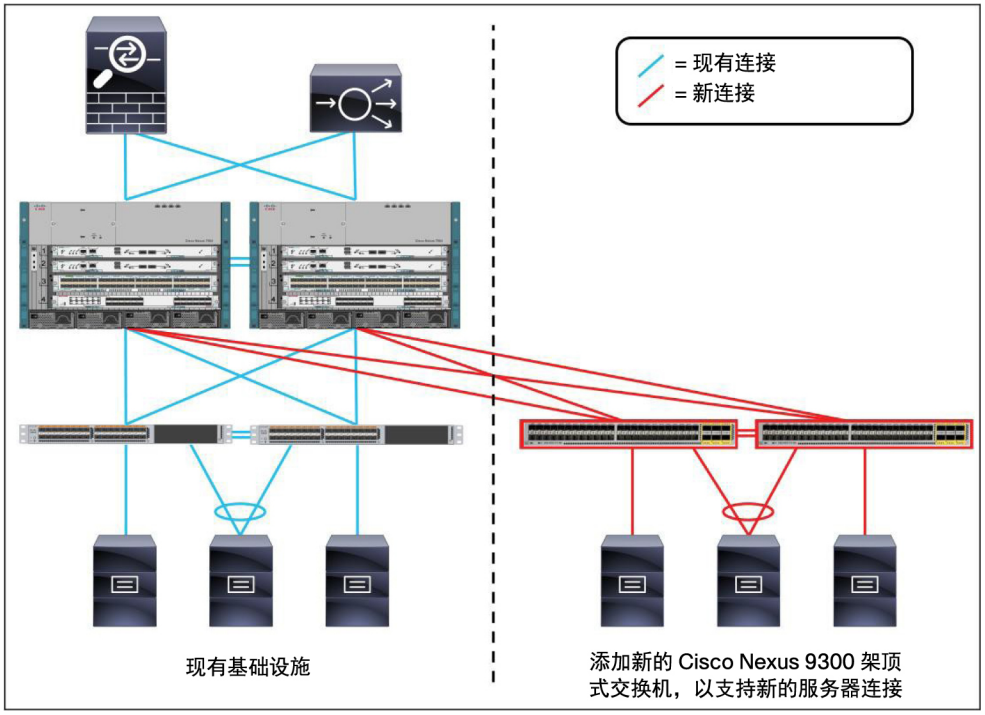
在随着应用增长而扩展或升级网络时，可以添加 Cisco Nexus 9000 系列交换机，作为新的数据中心汇聚 Pod。这模拟新 Pod 的传统插入方式。不需要移除或更改现有的服务器或第 4-7 层服务。为之前部分中介绍的每种设计提供了与现有网络集成的示例。

设计 A 集成

采用两台交换机的设计 A 拓扑可以作为新的数据中心接入和/汇聚 Pod 轻松插入。Cisco Nexus 9300 交换机显示为已连接到现有的数据中心汇聚交换机。然后在数据中心扩展时，新的服务器可以连接到 Cisco Nexus 9300 接入交换机。

可以使用标准协议将 Cisco Nexus 9300 平台轻松地与现有基础设施集成。就地的紧缩核心（汇聚）交换机仍可用于连接到第 4-7 层服务、外部网络和托管默认网关。虽然该现有网络描绘的是 Cisco Nexus 7000 和 5000 系列交换机，但现有网络可以是 Cisco Catalyst® 或其他供应商基础设施。

图 30. 现有数据中心内插入的两台交换机 Pod



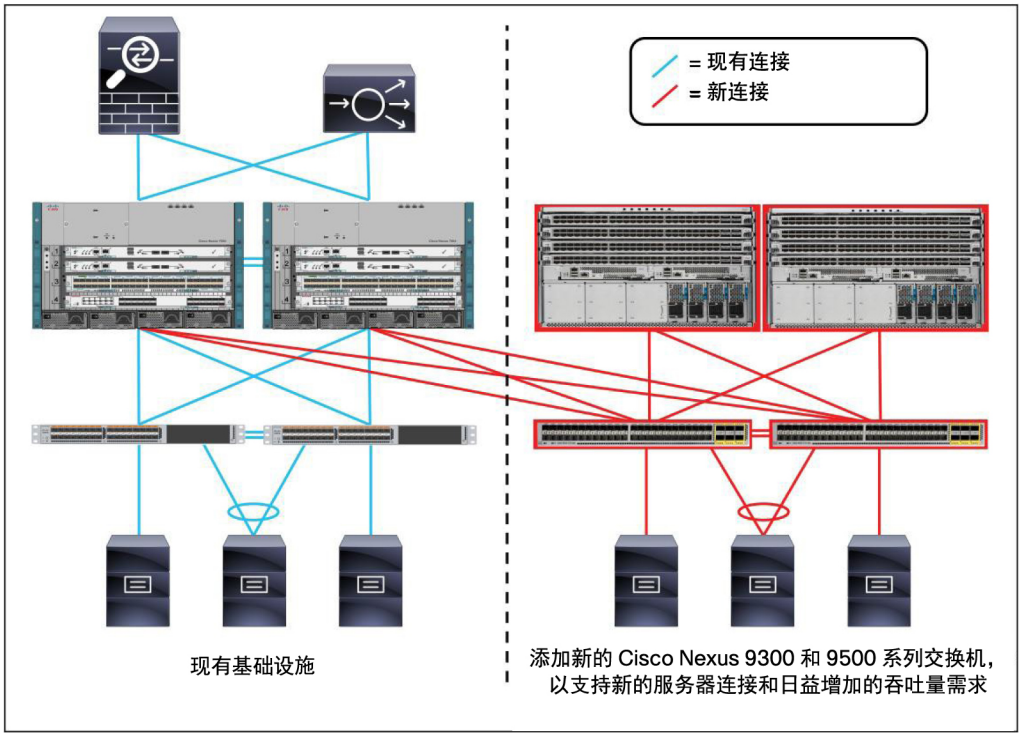
设计 B 集成

与设计 A 类似，采用两汇聚、两接入的设计 B 拓扑可以作为新的数据中心接入-汇聚 Pod 轻松插入。Cisco Nexus 9300 交换机显示为已连接到现有的数据中心汇聚交换机。然后在数据中心扩展时，新的服务器可以连接到 Cisco Nexus 9300 接入交换机。

可以使用标准协议将 Cisco Nexus 9300 平台轻松地与现有基础设施集成。就地的紧缩核心（汇聚）交换机仍可用于连接到第 4-7 层服务、外部网络和托管默认网关。虽然该现有网络描绘的是 Cisco Nexus 7000 和 5000 系列交换机，但现有网络可以是 Cisco Catalyst 或其他供应商基础设施。

随着较旧的交换机被逐步淘汰，第 4-7 层服务和默认网关最终可以迁移到新的 Nexus 9000 系列交换机。

图 31. 现有数据中心内插入的两汇聚、两接入 Pod

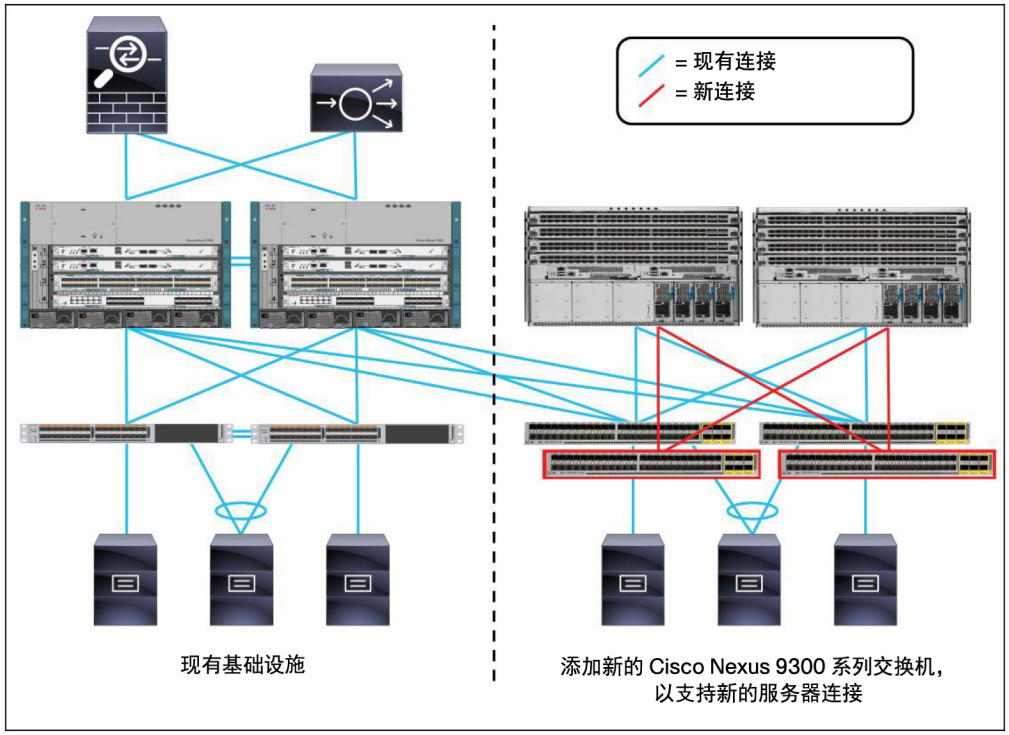


设计 C 和 D 集成

可以添加其他 Cisco Nexus 9300 枝叶接入交换机以支持不断增长的应用环境和数据中心。添加更多的 Cisco Nexus 9500 主干汇聚交换机可以满足不断增长的带宽需求，并且可以逐步淘汰老化的交换机。作为增长策略的一部分，可以将服务、网关和外部连接迁移到 Cisco Nexus 9000 系列交换机。

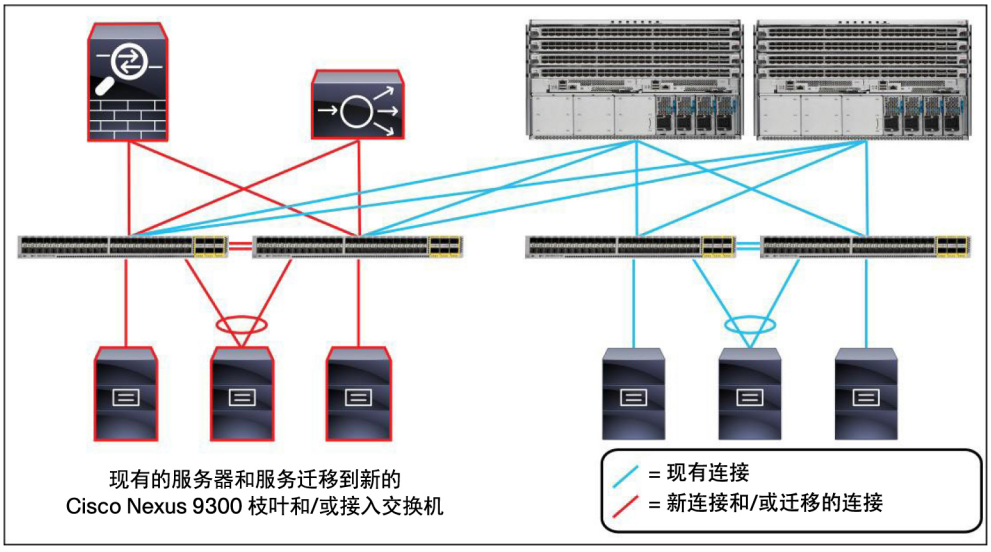
图 32 描绘了添加两台 Cisco Nexus 9300 枝叶和/或接入交换机，来满足应用和服务器的增长需求。

图 32. 将两台额外的 Cisco Nexus 9300 交换机集成到现有混合部署中



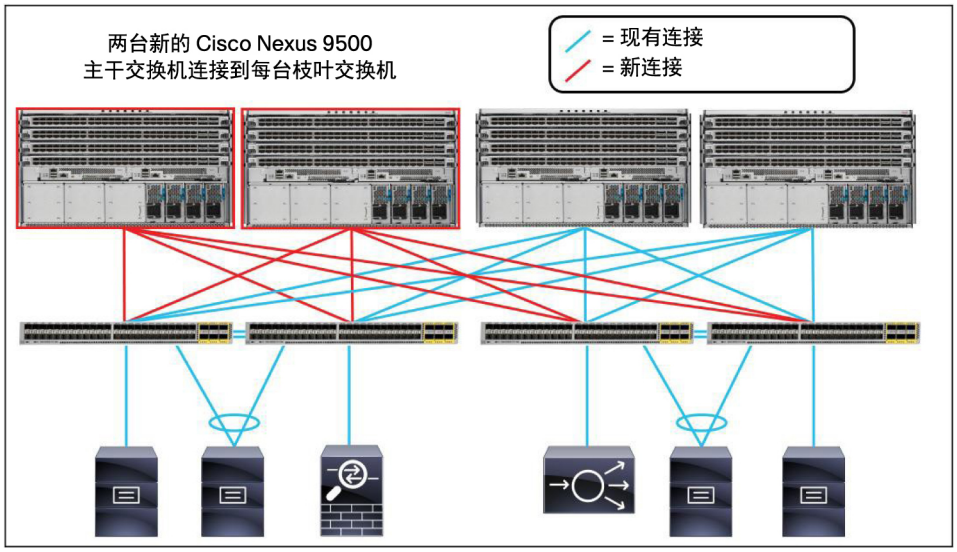
当现有设备可以逐步淘汰时，现有的服务器、服务和外部连接可以迁移到新的 Cisco Nexus 9300 枝叶和/或接入交换机，如图 33 所示。

图 33. 移除旧设备并将服务器和服务迁移到 Cisco Nexus 9000 系列交换机



随着应用和业务增长，可能需要更多带宽。图 34 描绘了再添加两台 Cisco Nexus 9500 主干和/或汇聚交换机。

图 34. 集成两台额外的 Cisco Nexus 9500 系列交换机



有关具体的 Cisco Catalyst 迁移细节的更多详情，请参阅 Migrate from Cisco Catalyst 6500 Series Switches to Cisco Nexus 9000 Series Switches（从 Cisco Catalyst 6500 系列交换机迁移到 Cisco Nexus 9000 系列交换机）白皮书。

交换矩阵扩展器支持

为使用现有硬件、提高接入端口密度和提高 1 千兆以太网端口可用性，可以在单宿主的直通配置中，将 Cisco Nexus 2000 系列交换矩阵扩展器连接到 Cisco Nexus 9300 平台。如果配置在 vPC 中，连接到交换矩阵扩展器的主机上行链路可以是主用/备用或主用/主用链路。

在撰写本文时，支持以下 Cisco Nexus 2000 系列交换矩阵扩展器：

- N2224TP
- N2248TP
- N2248TP-E
- N2232TM
- N2232PP
- B22HP

图 35. Cisco Nexus 2000 系列交换矩阵扩展器

如需了解最新的功能支持，请参阅 Nexus 9000 Software release notes（Nexus 9000 软件版本说明）。

还支持交换矩阵扩展器收发器 (FET)，以在 Cisco Nexus 2000 交换矩阵扩展器与其父交换机 Cisco Nexus 9300 之间提供经济高效的连接解决方案 (FET-10 Gb)。

有关 FET-10 GB 收发器的更多信息，请参阅 Nexus 2000 Series Fabric Extenders data sheet（Nexus 2000 系列交换矩阵扩展器产品手册）。

图中显示了支持的 Cisco Nexus 9000 至 Nexus 2000 交换矩阵扩展器拓扑。对于其他 Nexus 平台，可将思科交换矩阵扩展器技术（FEX 技术）看作父交换机 Cisco Nexus 9000 的逻辑远程线卡。每个思科 FEX 连接到一台父交换机。服务器应双宿至两个不同的交换矩阵扩展器。服务器上行链路可以在主用/备用 NIC 组合中，也可以在 vPC 中（如果在 vPC 域中设置父交换机 Cisco Nexus 9000）。

图 36. 支持的 Cisco Nexus 9000 系列交换机和交换矩阵扩展器设计（对于主用/备用服务器）

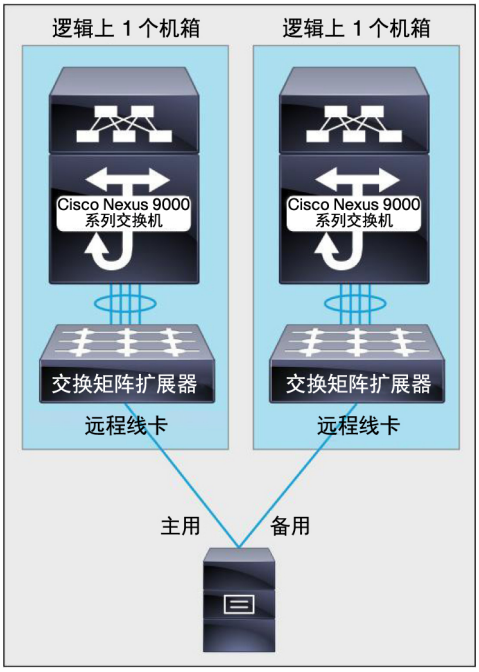
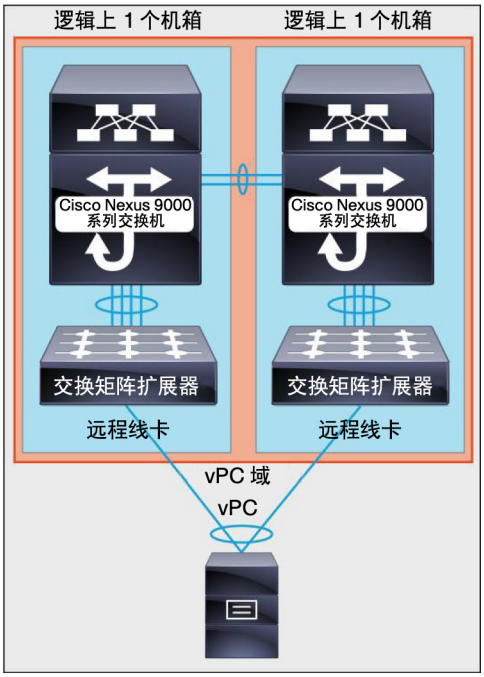


图 37. 支持的 Cisco Nexus 9000 系列交换机和交换矩阵扩展器设计（对于服务器 vPC）



有关详细信息，请参阅“Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches, Release 6.0”（Cisco Nexus 9000 系列交换机的 Cisco Nexus 2000 系列 NX-OS 交换矩阵扩展器配置指南 6.0 版）。

存储设计

现有的基于 IP 的存储（例如网络连接存储 [NAS] 或互联网小型计算机接口 [iSCSI] 存储）可与 Cisco Nexus 9000 交换矩阵集成。Cisco Nexus 9000 平台目前不支持光纤通道和以太网光纤通道 (FCoE)；但是，此部分演示了如何将它们设计在 Cisco Nexus 9000 平台旁边，以及如何随着添加的功能一起发展。请参考思科网站，获取有关未来对 FCoE N 端口虚拟化 (NPV) 提供的支持的更新信息。如果客户希望为每台服务器使用单独、专用的存储连接，那么客户可以使用电缆将存储连接与其物理存储网络相连，并使用电缆将生产 IP LAN 连接与 Nexus 9000 相连。

专用的物理存储网络可以使用基于 IP 的存储，例如 iSCSI 或 NAS，也可以由光纤通道或 FCoE 网络组成。无论使用的协议是什么，此设计不需要对现有存储布线进行任何更改。图 38 举例说明了 SAN 流量的单独、专用的存储网络，LAN 流量通过 Nexus 9000 交换矩阵。

图 38. 用于 LAN 和单独的物理 SAN 的 Cisco Nexus 9000 系列交换机

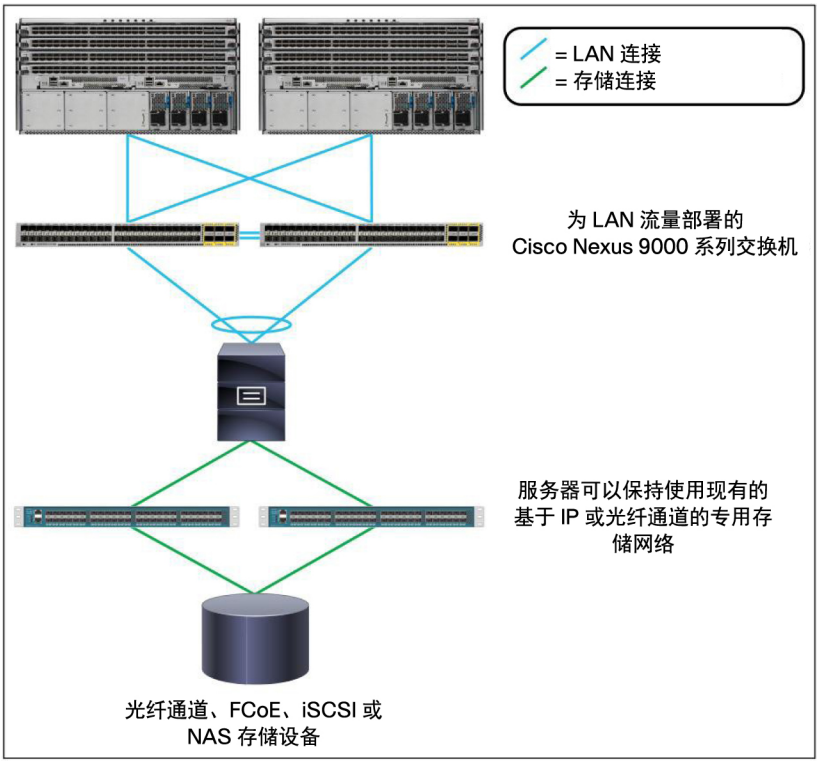
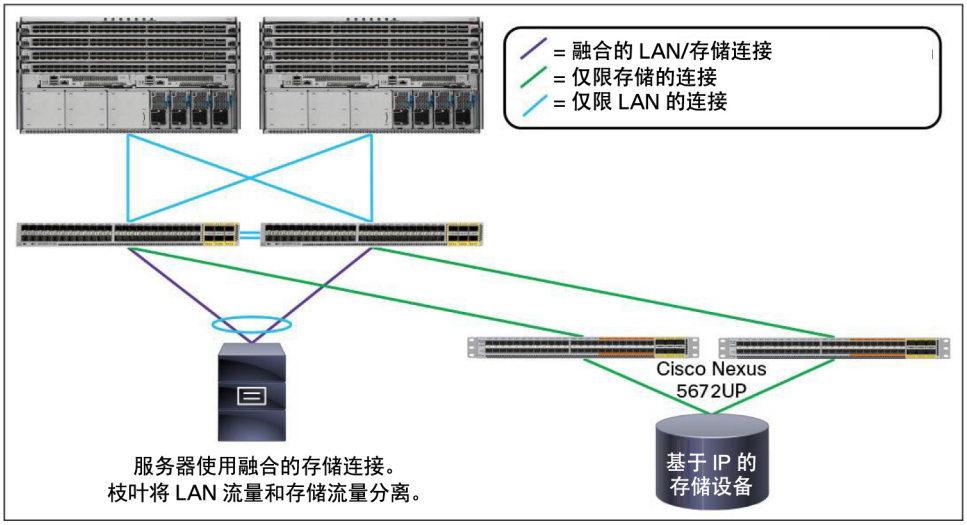


图 38 显示了新的思科 MDS 9148S 多层交换矩阵交换机。思科 MDS 9148 交换矩阵交换机是高度经济实惠、多用途、易于管理的多协议存储网络交换机，适合入门级和部门 SAN 使用。思科 MDS 9148S 交换矩阵交换机基于芯片内交换的思科存储网络 ASIC，每个端口提供 16 Gbps 的专用光纤通道带宽。思科 MDS 9148S 光纤交换机以 12 端口的基本配置提供，通过按需的“随增长，随投资”12 端口激活许可证可以扩展到 48 个端口。还提供完全许可的 48 端口配置。思科 9148S 交换矩阵交换机为融合交换矩阵启用可扩展且灵活的 SAN 架构，包括通过 Cisco FabricPath 支持 FCoE、FCoE-FEX 和 FCoE。

有关思科 MDS 9148S 多层交换矩阵交换机的更多信息，请参阅思科的 Storage Networking（存储网络）网页。

如果使用基于 IP 的存储（例如 iSCSI 或 NAS），可通过 Cisco Nexus 9000 系列交换机实现融合存储交换矩阵设计，以减少所需的布线、交换机端口、交换机数量和适配器数量，并显著节约能耗。所有服务器都连接到 Cisco Nexus 9300 平台枝叶（接入交换机），传输 LAN 流量和基于 IP 的存储流量。存储设备也可以连接到枝叶，或者也可以保持连接到现有基础设施。图 39 和图 40 显示了两个选项。

图 39. 在 Cisco Nexus 9300 平台上使用基于 IP 的存储为服务器提供融合接入



Cisco Nexus 9372 枝叶接入交换机分离要发送到主干汇聚交换机的 LAN 流量，并将基于 IP 的存储流量发送到专用于存储流量的交换机。虽然可以使用许多交换机，但是图 40 重点介绍了 Cisco Nexus 5672UP 交换机。

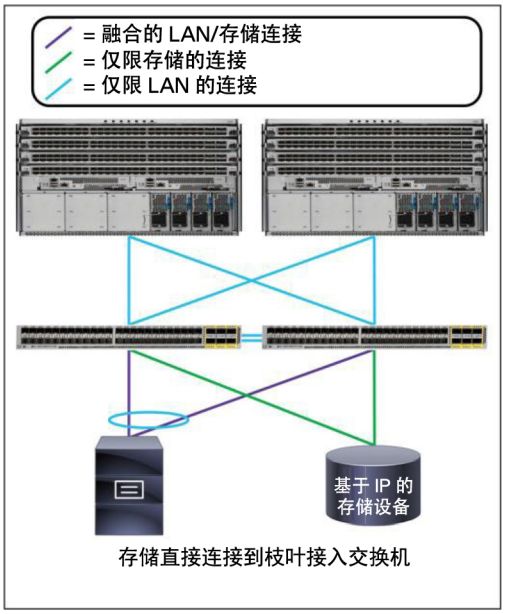
Cisco Nexus 5600 系列交换机是业界领先的 Cisco Nexus 5000 系列数据中心服务器接入交换机的第三代。Cisco Nexus 5600 平台是业界最广泛采用的 Cisco Nexus 5500 交换机的后续产品，它保持所有现有的 Cisco Nexus 5500 功能，其中包括 LAN/SAN 融合（统一端口、FCoE）、交换矩阵扩展器和交换矩阵路径，但除此之外，它还通过真正的 40 千兆以太网支持来提供集成的线速第 2 层和第 3 层，并且提供思科动态交换矩阵自动化创新、使用通用路由封装 (NVGRE) 的网络虚拟化、VXLAN 桥接和路由能力、网络可编程性与可视性、深度缓冲区，并为高度虚拟化、自动化的云环境提供显著提高的规模和性能。

图 40. Cisco Nexus 5672UP 交换机

有关更多信息，请参阅 Cisco Nexus 5600 Platform Switches Data Sheet（Cisco Nexus 5600 平台交换机产品手册）。

在图 41 描绘的设计中，服务器和基于 IP 的存储设备直接连接到枝叶接入交换机，从而减少跳数和设备数。

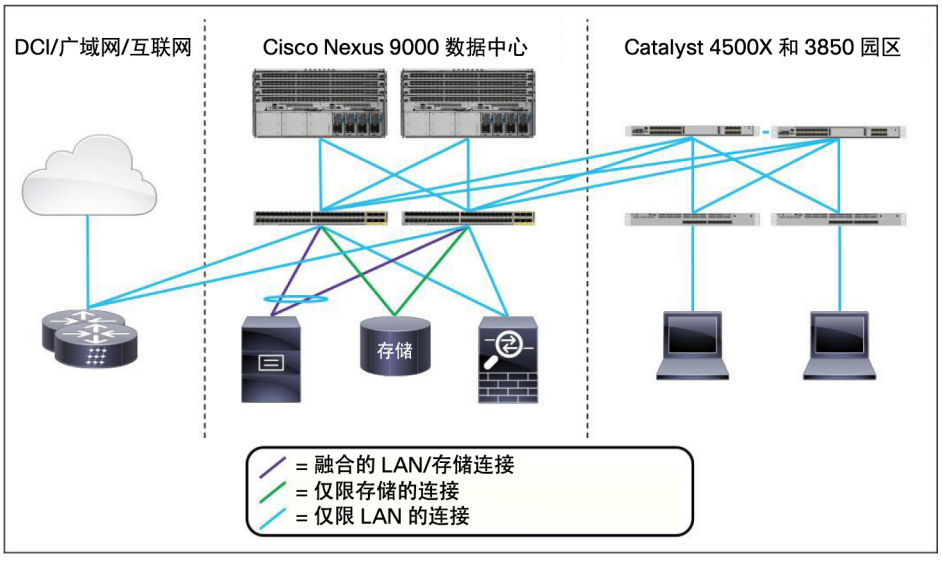
图 41. 在 Cisco Nexus 9300 平台上为服务器和基于 IP 的存储设备提供融合接入



最终状态拓扑

图 42 是一个简图，显示了与现有数据中心集成的最终状态设计的一个示例。该设计包括两台 Cisco Nexus 9372 交换机、两台 Cisco Nexus 9504 交换机、基于 IP 的存储设备、一台思科 ASA 防火墙设备、与园区 Cisco Catalyst LAN 环境的连接以及与 WAN 路由器的连接。请注意，所有设备都连接到 Cisco Nexus 9300 枝叶接入交换机。

图 42. 最终状态广域网、数据中心和园区网络示例



示例：Cisco Nexus 9000 系列设计和配置

此部分使用实际的设备介绍 Cisco Nexus 9000 系列设计的一个示例，这些设备包括 Cisco Nexus 9508 交换机、Nexus 9396 交换机、VMware ESXi 服务器和独立的裸机服务器以及思科 ASA 防火墙。已在思科实验室中测试此拓扑，以验证和演示 Cisco Nexus 9000 解决方案。

您的确切配置可能有所不同。本部分的目的是提供一个网络设计和配置示例，包括本白皮书前面部分讨论的功能。请务必参考思科配置指南，获取最新的信息。

使用的术语和交换机名称引用“枝叶”和“主干”，但相同的配置可以应用于接入-汇聚设计。

本部分包括以下功能的解释和最终状态配置：

- 基本网络设置：
  - VLAN 和中继
  - IP 寻址
- ECMP 路由基础设施：
  - EIGRP
- 服务器 NIC 组合：
  - 虚拟 PortChannel (vPC)
- 重叠：
  - 虚拟可扩展局域网 (VXLAN)
  - 组播
- 服务：
  - 思科 ASA 防火墙
- 管理：
  - 思科数据中心网络管理器 (DCNM)
- 云就绪性

硬件和软件规格

- 两台 Cisco Nexus N9K-C9508 交换机（8 个插槽），每台交换机中具有以下组件：
  - 一个 N9K-X9636PQ (36p QSFP 40G) 以太网模块
  - 六个 N9K-C9508-FM 交换矩阵模块
  - 两个 N9K-SUP-A 管理引擎模块
  - 两个 N9K-SC-A 系统控制器
- 两台 Cisco Nexus 9396PX 系列交换机 (48p SFP+ 1/10G)，每台交换机中具有以下扩展模块：
  - 一个 N9K-M12PQ (12p QSFP 40G) 以太网模块
- 三台思科 UCS C 系列服务器（对于较小型的部署，可以替换为思科 UCS 快捷版服务器）。有关服务器选项的更多信息，请参阅 Cisco Unified Computing System Express（思科统一计算系统快捷版）。
- 一台思科 ASA 5510 防火墙设备

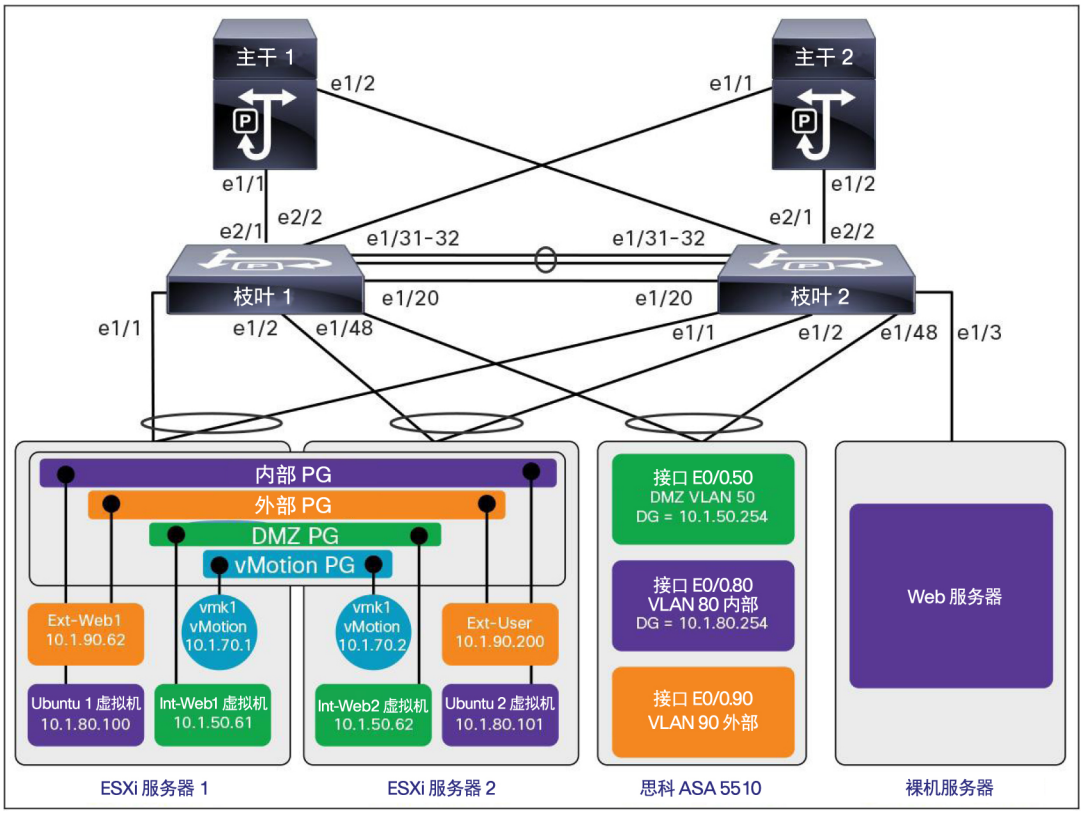
本设计中使用的 Cisco Nexus 9000 交换机运行 Cisco NX-OS 6.1(2)I2(3) 版本。使用的 VMware ESXi 服务器运行 ESXi 5.1.0 版本 799733。思科 ASA 运行 8.4(7) 版本。

基本网络设置

在这个简单拓扑中，VLAN 50 是隔离区 (DMZ)，VLAN 70 用于 vMotion，VLAN 80 是内部生产 Web 服务器，VLAN 90 用于外部流量。物理接口 eth2/1 和 eth2/2 连接到主干。接口 eth1/1 连接到 VMware ESXi 服务器，接口 eth1/48 连接到思科 ASA 5510 防火墙设备（后面显示配置）。以下逻辑拓扑图中显示了该配置（图 43）。

图 43. 拓扑示例中使用的 VLAN

图 44. 实验室拓扑图和 VLAN 用途



提供了经过实验室测试的拓扑中的枝叶交换机的接口配置示例。其他枝叶和主干以类似方式配置。解释性的备注以内嵌的斜体形式提供，前面带有感叹号(!)。Cisco NX-OS 命令以粗体显示。

图 45. 基本 VLAN 和接口配置

```
! Create and (optionally) name VLANs

Leaf1# configure terminal
Leaf1(config)# vlan 50,70,80,90
Leaf1(config-vlan)# vlan 50
Leaf1(config-vlan)# name DMZ
Leaf1(config-vlan)# vlan 70
Leaf1(config-vlan)# name vmotion
Leaf1(config-vlan)# vlan 80
Leaf1(config-vlan)# name internal
Leaf1(config-vlan)# vlan 90
Leaf1(config-vlan)# name external

! Configure Layer 3 spine-facing interfaces

Leaf1(config-vlan)# interface Ethernet2/1
Leaf1(config-if)# description to Spine1
Leaf1(config-if)# no switchport
Leaf1(config-if)# ip address 10.1.1.2/30
Leaf1(config-if)# no shutdown

Leaf1(config-if)# interface Ethernet2/2
Leaf1(config-if)# description to Spine2
Leaf1(config-if)# no switchport
Leaf1(config-if)# ip address 10.1.1.10/30
Leaf1(config-if)# no shutdown

! Configure Layer 2 server and service-facing interfaces
! (Optionally) Limit VLANs and use STP best practices

Leaf1(config-if)# interface Ethernet1/1-2
Leaf1(config-if)# switchport
Leaf1(config-if)# switchport mode trunk
Leaf1(config-if)# switchport trunk allowed vlan 50,70,80,90
Leaf1(config-if)# spanning-tree bpduguard enable
Leaf1(config-if)# spanning-tree port type edge trunk
Warning: Edge port type (portfast) should only be enabled on ports connected to a
single host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when edge port type (portfast) is enabled, can cause temporary bridging
loops. Use with CAUTION.
Leaf1(config-if)# no shutdown
```

```
Leaf1(config-if)# interface Ethernet1/1
Leaf1(config-if)# description to Server1
Leaf1(config-if)# interface Ethernet1/2
Leaf1(config-if)# description to Server2

Leaf1(config-if)# interface Ethernet1/48
Leaf1(config-if)# description to ASA
Leaf1(config-if)# switchport
Leaf1(config-if)# switchport mode trunk
Leaf1(config-if)# switchport trunk allowed vlan 50,70,80,90
Leaf1(config-if)# no shutdown
```

有关基本配置的更多信息，请参阅“Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 6.0”（Nexus 9000 系列 NX-OS 接口配置指南 6.0 版）。

如需最新的 Cisco NX-OS 版本指南，请参阅 Cisco Nexus 9000 系列交换机配置指南网页。

ECMP 路由设计

利用控制平面中使用的第 3 层动态路由协议可实现最佳的流量路由和等价多路径，并减少交换机之间的交换矩阵中对生成树的需求。生成树仍需要在其他非交换矩阵接口上运行，以阻止传统以太网环境中的环路。每台交换机之间的所有路径主动转发流量。

思科增强型内部网关路由协议 (EIGRP) 用于拓扑示例中。使用增强型第 3 层许可证还可以在 Cisco Nexus 9300 和 9500 平台上支持开放最短路径优先 (OSPF) BGP、中间系统到中间系统 (IS-IS) 和静态路由。EIGRP 快速收敛和出色的可扩展性。由于每台枝叶和/或接入交换机连接到每台主干和/汇聚交换机，因此 EIGRP 将负载平衡到所有等价路径。

下面的图 46 显示了经过实验室测试的拓扑中的枝叶交换机的 EIGRP 配置示例。其他枝叶和主干以类似方式配置。

图 46. EIGRP 配置

```
! Enable the EIGRP feature
! Configure global EIGRP process and (optional) router ID

Leaf1(config)# feature eigrp
Leaf1(config)# router eigrp 1
Leaf1(config-router)# router-id 1.1.1.33

! Enable the EIGRP process on spine-facing interfaces

Leaf1(config-router)# interface Ethernet2/1-2
Leaf1(config-if)# ip router eigrp 1
```

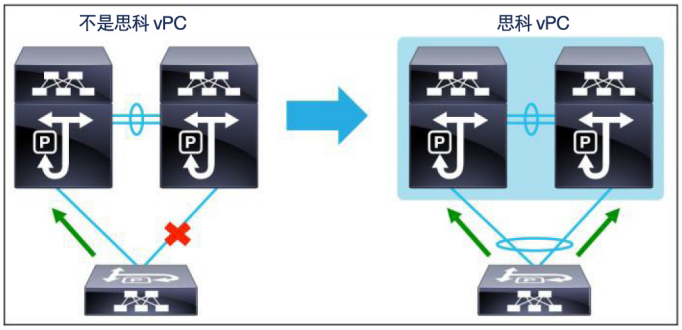
有关配置 EIGRP 的更多信息，请参阅“Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 6.0”（Cisco Nexus 9000 系列 NX-OS 单播路由配置指南 6.0 版）。

服务器 NIC 组合设计和配置

现代的应用以及由于 CPU 和内存空间进步而日益提高的虚拟机密度推动服务器带宽需求，许多服务器需要 10 GB 连接。理想情况下，每台服务器双宿至两台不同的物理交换机。通常，其中一个连接主动转发流量，另一个连接则备用。虽然此设计可在交换机发生故障的情况下提供冗余，但是备用或被阻止的连接会消耗潜在的带宽。

思科 vPC 允许来自一个思科 PortChannel 的设备中的连接在一对以特殊对等关系设置的两台不同 Cisco Nexus 交换机上终止。思科 vPC 提供第二层多路径，在保持冗余的同时提高带宽。可以在一个思科 vPC 中设置任何支持思科 PortChannel 的设备，该思科 vPC 连接到思科 vPC 域中的一对交换机，并且该设备不知道它已配置为一种特殊类型的 PortChannel。

图 47. 传统以太网转发路径与思科 vPC 主用/主用转发路径对比



思科 vPC 提供以下优势：

- 允许单个设备使用连接到两台上游 Cisco Nexus 交换机的思科 PortChannel。
- 消除生成树阻止的端口。
- 提供无环路拓扑。
- 使用所有可用的上行链路带宽。
- 在链路或交换机出现故障时提供快速收敛。
- 通过标准的思科 PortChannel 机制提供链路级的恢复能力。
- 通过连接到两台不同的物理交换机帮助确保高可用性。

思科 vPC 域包括两台 Cisco Nexus 对等交换机（设计示例中的 Cisco Nexus 9000 系列交换机）、用作对等体间心跳的思科 vPC 对等保持连接链路、vPC 对等链路（用于交换控制流量、孤立流量和多目标流量），以及思科 vPC 域中连接到下游设备的所有 PortChannel。您在每台交换机上只能有一个 vPC 域 ID，并且每个思科 vPC 域只能有两台交换机。

在拓扑示例中，思科 vPC 域中设置两台枝叶（接入）交换机。思科 ASA 防火墙设备和大多数服务器通过思科 vPC 连接到枝叶（接入交换机）。一些旧服务器单宿至不属于思科 vPC 一部分的交换机。最佳做法是所有设备都通过思科 vPC 连接到两台交换机，但并不要求这样做。

同一域中的思科 vPC 对等交换机需使用相同的域编号。此外，给定设备的思科 vPC 编号在两端必须匹配。思科 PortChannel 编号在本地很重要，并且不需要在两端匹配。

提供了经过实验室测试的拓扑中的枝叶交换机的思科 vPC 配置示例。另一台枝叶交换机以类似方式配置。思科 vPC 是第 2 层 PortChannel，因此无需在主干交换机上配置思科 vPC 域，因为它们通过第 3 层接口连接到枝叶。

遵循思科 vPC 设计的最佳实践至关重要。思科强烈建议阅读 vPC Best Practices Design Guide（vPC 最佳实践设计指南）。但是应实施的关键最佳实践包括：

- **域、对等链路、对等保持连接和成员接口最佳实践**
  - 不同的思科 vPC 域必须使用不同的思科 vPC 域 ID 成员。
  - 域中的两个对等体上的所有思科 vPC 1 类一致性检查必须匹配。
  - 域中的两个对等体上的所有思科 vPC 2 类一致性检查应匹配。
  - 应以相同的方式在两台对等交换机上配置思科 vPC 成员接口。
  - 在与思科 vPC 相关的所有思科 PortChannel 上使用链路汇聚控制协议 (LACP)。
  - 在思科 vPC 对等链路和成员端口上，以正常模式启用单向链路检测 (UDLD)。
  - 将组播与思科 vPC 配合使用时，务必启用 PIM 预构建最短路径树 (SPT)。
  - 理想情况下，对等保持连接心跳链路应为专用 (VRF) 中的一对直连第 3 层接口。
  - 使用思科 vPC 互连最多两个数据中心。如果需要互连的数据中心超过两个，请使用重叠传输虚拟化 (OTV)。
  - 在两个不同线卡上构建对等链路以增加冗余。不要在对等链路连接的对等交换机之间插入任何设备。
  - 将思科 vPC VLAN 和非思科 vPC 的 VLAN 分离到不同的思科 PortChannel 上。
  - 为简化配置、监控和故障排除，请使用相同的思科 vPC ID 和 PortChannel 编号。
  - 如果可能，请将连接的每台设备双连至思科 vPC 域。
  - 始终在思科 vPC 域中启用 vPC 对等网关（即同时在两台思科 vPC 对等设备上配置对等网关），即使不存在使用此功能的终端设备（不对其默认 IP 网关执行标准 ARP 请求的设备）。启用此功能没有副作用。
  - 请务必同时在两台 vPC 对等设备上启用思科 vPC ARP 同步。
  - 如果在 vPC 对等链路出现故障时，连接至思科 vPC 域的单连设备需要断开与网络的连接，请使用思科 vPC 孤立端口挂起命令。
- **HSRP-VRRP 最佳实践：**
  - 以主用-主用模式（数据平面角度）运行热备用路由器 (HSRP) 和虚拟路由器冗余协议 (VRRP) 时，可放弃使用主动计时器：使用默认的 HSRP - VRRP 计时器。
  - 将与第一跳冗余协议 (FHRP) 和 VRRP 相关联的交换机虚拟接口 (SVI) 定义为被动路由接口，以避免在思科 vPC 对等链路上形成路由邻接。
  - 将思科 vPC 主要对等设备定义为主用 HSRP-VRRP 实例，将思科 vPC 次要对等设备定义为备用 HSRP-VRRP（从控制平面的角度），以便于操作。

- 在配置了 HSRP-VRRP 的 VLAN 接口上禁用 IP 重定向（命令是 no IP redirect）。这是与 HSRP-VRRP 相关的通用最佳实践。
- 请勿在思科 vPC 域中使用 HSRP-VRRP 对象跟踪。

- **生成树最佳实践：**
  - 请勿禁用生成树。
  - 对于大型第 2 层域，请使用 MST。
  - 在同一第 2 域中的所有设备上，使用相同版本的生成树。
  - 在思科 vPC 成员端口上配置 VLAN 修剪。
  - 在网络的汇聚层（汇聚思科 vPC 域）保留 STP 根功能。
  - 对于每台思科 vPC 对等设备，请在连接到接入设备的端口上配置根防护。
  - 配置思科 vPC 对等链路时，默认启用网桥保障。请勿在思科 vPC 对等链路上禁用网桥保障。
  - 将思科 vPC 成员端口配置为 SPT 正常端口类型（不在链路上使用网桥保障）。
  - 在面向主机的接口上配置思科快速端口（边缘端口类型），以避免端口转换到运行状态时缓慢地进行 STP 收敛（30 秒或更长时间）。
  - 在面向主机的接口上配置桥接协议数据单元 (BPDU) 防护，以阻止从主机发送的所有 BPDU（接收 BPDU 的接入交换机端口将进入 errdisable 模式）。
  - 请始终将思科 vPC 域定义为该域中所有 VLAN 的 STP 根（将汇聚 vPC 对等设备配置为主要 STP 根和次要 STP 根）。通过在连接至另一第 2 层交换机的思科 vPC 对等设备端口上实施 STP 根防护来实施此规则。

要升级接入层而不中断 vPC 中的双宿主机，请完成以下任务：

- 首先升级 vPC 主要对等交换机。升级期间，该交换机将重新加载。该交换机重新加载后，vPC 中的下游设备会检测与 vPC 主要对等交换机的连接的丢失情况，并开始将这些链路上的流量转发至另一对等交换机。
- 确认 vPC 主要对等交换机的升级已成功完成。升级完成后，交换机将恢复 vPC 对等和所有 vPC 链路。
- 确认 vPC 域完全重新融合之后，请重复同一过程以升级其他对等交换机。此交换机将在升级过程中重新加载。在重新加载期间，第一个（已升级）交换机将转发所有进出下游设备的流量。
- 确认第二个交换机的升级已成功完成。此升级结束时，完整的 vPC 对等关系已建立，并且升级完成。

图 48 显示了思科 vPC 配置。图 49 显示了分支交换机上的思科 vPC 配置。

图 48. 思科 vPC 配置示例

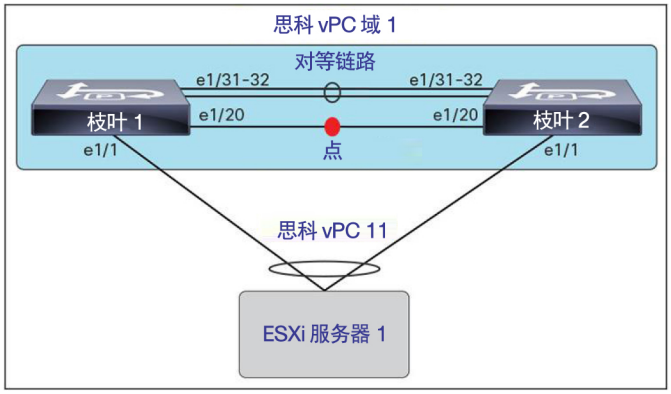


图 49. 思科 vPC 域和设备配置

```
! Configure UDLD in normal mode per best practices

Leaf1(config)# feature udld

! Prepare peer-keepalive heartbeat interface and VRF

Leaf1(config)# vrf context KEEPALIVE
Leaf1(config)# interface Ethernet1/20
Leaf1(config)# vrf member KEEPALIVE
Warning: Deleted all L3 config on interface Ethernet1/20
Leaf1(config)# ip address 192.168.99.1
Leaf1(config)# no shutdown

! Enable feature and create a vPC domain

Leaf1(config)# feature vpc
Leaf1(config)# vpc domain 1

! Set peer keepalive heartbeat source and destination

Leaf1(config-vpc-domain)# peer-keepalive destination
192.168.99.2 source 192.168.99.1 vrf KEEPALIVE

! Automatically and simultaneously enable the following
! best practice commands using the mode auto command: peer-
! gateway, auto-recovery, ip arp synchronize, and ipv6 nd
! synchronize.

Leaf1(config-vpc-domain)# mode auto

! Create the peer-link Port Channel and add to domain

Leaf1(config-vpc-domain)# feature lacp
Leaf1(config)# interface Ethernet1/31-32
Leaf1(config-if-range)# channel-group 1 mode active
Leaf1(config-if-range)# interface port-channel 1
Leaf1(config)# switchport
Leaf1(config)# switchport mode trunk
Leaf1(config)# switchport trunk allowed vlan 50,70,80,90
Leaf1(config)# vpc peer-link
Please note that spanning tree port type is changed to "network" port type on vPC
peer-link. This will enable spanning tree Bridge Assurance on vPC peer-link
provided the STP Bridge Assurance (which is enabled by default) is not disabled.
```

```
Leaf1(config)# no shutdown

! Configure best practice Spanning Tree features on vPC
! Create a Port Channel and vPC for a server
! The vPC #11 must match on the other peer for the server

Leaf1(config)# interface Ethernet1/1
Leaf1(config)# channel-group 11 mode active
Leaf1(config)# interface port-channel 11
Leaf1(config)# spanning-tree port type edge
Leaf1(config)# spanning-tree bpdu guard enable
Leaf1(config)# vpc 11

! Repeat vPC configuration for any additional devices
! connected to the vPC domain
```

有关更多信息，请参阅“Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 6.0”（Cisco Nexus 9000 系列 NX-OS 接口配置指南 6.0 版）的 Configuring vPCs（配置 vPC）一章。

重叠设计和配置

商业设计示例中部署的虚拟重叠通过第 3 层 EIGRP 网络提供第 2 层可达性。本部分讨论 VXLAN 基础、如何设置组播路由以支持 VXLAN，以及如何在 Cisco Nexus 9000 系列交换机上配置 VXLAN。VXLAN 在 Cisco Nexus 9000 交换机上不是必需的，但是，它在路由基础设施中提供可选的重叠。虚拟 PortChannel 和路由汇聚是同样有效的设计。

为什么实施 VXLAN？

VXLAN 的特点为选择重叠。VXLAN 是在第 3 层网络上运行的第 2 层重叠，解决传统网络中存在的一些痛点。许多常用数据中心应用需要第 2 层邻接进行通信。例如，虚拟机工作负载移动性和某些群集应用必须通过专用 VLAN 或子网通信，且无法路由。但是，构建大型第 2 层网段会产生大型广播域并增大不良事件（例如，SPT 重新融合）的范围。生成树协议会因为预防环路而阻止链路，这会消耗带宽并从而增加过载。此外，VLAN 最多只可扩展到 4094 个网段，交换机保留许多 VLAN 供内部使用。

VXLAN 旨在提供与传统 VLAN 相同的第 2 层可达性、分段和服务，但它可突破许多限制。与 VLAN 相比，VXLAN 提供以下优势：

- 可在整个数据中心中灵活地安置多租户网段：它提供了一个解决方案以通过底层共享网络基础设施扩展第 2 层网段，以便可在数据中心内的物理 Pod 间安置和移动租户工作负载。
- 更高的扩展性可处理更多第 2 层网段：VLAN 使用 12 位 VLAN ID 以处理第 2 层网段，从而导致最多只能扩展至 4094 个 VLAN。VXLAN 使用 24 位网段 ID，又称为 VXLAN 网络标识 (VNID)，它允许多达 1600 万个 VXLAN 网段共存于同一管理域。

- 更好地利用底层基础设施中的可用网络路径：VLAN 使用 SPT 来预防环路，它会阻止冗余路径从而导致网络中的网络链路使用率不到一半。相比之下，VXLAN 包通过基于第 3 层报头的底层网络传输，可以充分利用第 3 层路由、ECMP 路由和链路汇聚协议以使用所有可用路径。

可在基于虚拟机监控程序的虚拟交换机上实施 VXLAN 以允许可扩展可重复的虚拟机部署，也可在充当网关的物理交换机上实施 VXLAN 以将 VXLAN 网段桥接回 VLAN 网段。

有关更多信息，请参阅 VXLAN Overview: Cisco Nexus 9000 Series Switches（VXLAN 概述：Cisco Nexus 9000 系列交换机）。

VXLAN 如何工作？

为在第 3 层基础设施中扩展第 2 层网络，VXLAN 使用 MAC-in-UDP（用户数据报协议）封装和基于 IP 传输的无状态隧道。托管通道并执行数据包封装和解封的设备称为 VXLAN 隧道终端 (VTEP)。充当硬件 VXLAN 网关时，Cisco Nexus 9000 VTEP 将 VXLAN 网段和传统 VLAN 网段组合到一个公共第 2 层域中。

在 VXLAN 中，Cisco Nexus 9000 VTEP 有两种接口：连接至服务器、设备或其他交换机的传统第 2 层以太网接口，以及称为网络虚拟化边缘 (NVE) 且绑定至环回接口的第 3 层 IP 接口。NVE 接口有多项功能：

- 在传输网络上唯一标识 VTEP（交换机）。
- 封装和解封 VXLAN 帧。
- 发现远程 VTEP（交换机）以获取它的已配置 VXLAN 网段。
- 了解要用于转发查找的远程 MAC 地址至 VTEP 映射。

VTEP 的源和目标 IP 用于通过底层传输网络转发 VXLAN 封装的流量（将流量从入口的源分支交换机路由至出口的目标分支交换机）。VXLAN 网段独立于底层网络拓扑，并且 VTEP 之间的底层网络拓扑独立于 VXLAN 重叠。

在封装时，VTEP 采取原始第 2 层帧并添加 8 字节 VXLAN 报头。此外，还会添加 UDP、IP 和 MAC 报头。VXLAN 报头中的主要字段是一个 24 位的 VXLAN 网络标识符 (VNID)。每个 VNID 表示唯一的 VXLAN 网段 ID。

组播注意事项

VXLAN 使用组播来缩小同一 VXLAN 网段中的主机的洪流范围。组播组用于传输广播、未知单播和组播流量，发现远程 VTEP（交换机），了解远程主机 MAC 地址及每个 VXLAN 网段的 MAC 至 VTEP 映射。作为配置的一部分，每个 VLAN 至 VXLAN 网段映射至一个组播组。

因此，必须在传输网络中配置组播路由以支持 VXLAN。启用组播支持需要 PIM 和交汇点配置。每个 VXLAN 网段映射至传输网络中的一个组播组，每个 VTEP 通过 IGMP 加入。

在拓扑结构示例中，使用任意源组播 (ASM) 的 PIM 稀疏模式用于组播路由，以通告组成员资格和构建组播分布树。组播源发现协议 (MSDP) 用于创建任意播交汇点配置以提供交汇点冗余和负载分摊。VXLAN 不要求使用 MSDP，但要求存在交汇点。

主干（汇聚）组播配置

此处的图 50 中显示了经过实验室测试的拓扑中的主干交换机的组播配置示例。另一台主干交换机以类似方式配置。分支以不同方式配置，稍后将显示。

图 50. 主干 PIM 和 MSDP 组播配置

```
! Enable PIM and MSDP to turn on multicast routing

Spine1(config)# feature pim
Spine1(config)# feature msdp

! Enable PIM on the spine-facing interfaces
! EIGRP should already be enabled on the interfaces

Spine1(config)# interface Ethernet1/1-2
Spine1(config-if-range)# ip pim sparse-mode

! Configure the Rendezvous Point IP address for the ASM
! group range 239.0.0.0/8 to be used by VXLAN segments

Spine1(config-if-range)# ip pim rp-address 10.2.2.12 group-list 239.0.0.0/8

! Configure loopbacks to be used as redundant RPs with
! the other spine switch. L0 is assigned a shared RP IP
! used on both spines. L1 has a unique IP address.
! Enable PIM and EIGRP routing on both loopback interfaces.

Spine1(config)# interface loopback0
Spine1(config-if)# ip address 10.2.2.12/32
Spine1(config-if)# ip router eigrp 1
Spine1(config-if)# ip pim sparse-mode

Spine1(config-if)# interface loopback1
Spine1(config-if)# ip address 10.2.2.1/32
Spine1(config-if)# ip router eigrp 1
Spine1(config-if)# ip pim sparse-mode
```

```
! Configure MSDP sourced from loopback 1 and the peer spine
! switch's loopback IP address to enable RP redundancy

Spine1(config-if)# ip msdp originator-id loopback1
Spine1(config)# ip msdp peer 10.2.2.2 connect-source loopback1
```

有关 PIM 的更多信息，请参阅 Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS 组播路由配置指南 6.0 版）中的“Configuring PIM（配置 PIM）”一章。

有关 MSDP 的更多信息，请参阅 Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS 组播路由配置指南 6.0 版）中的“Configuring MSDP（配置 MSDP）”一章。

枝叶（接入）组播配置

分支交换机使用主干汇聚上配置的组播组和交汇点。分支交换机必须已在面向主干的接口上配置组播，并指向交汇点 IP 地址。

图 51 说明了主干和分支上的组播设置。此处显示了经过实验室测试的拓扑中的分支交换机的组播配置示例。另一台分支交换机（图 52）以类似方式配置。

图 51. 主干和分支组播图

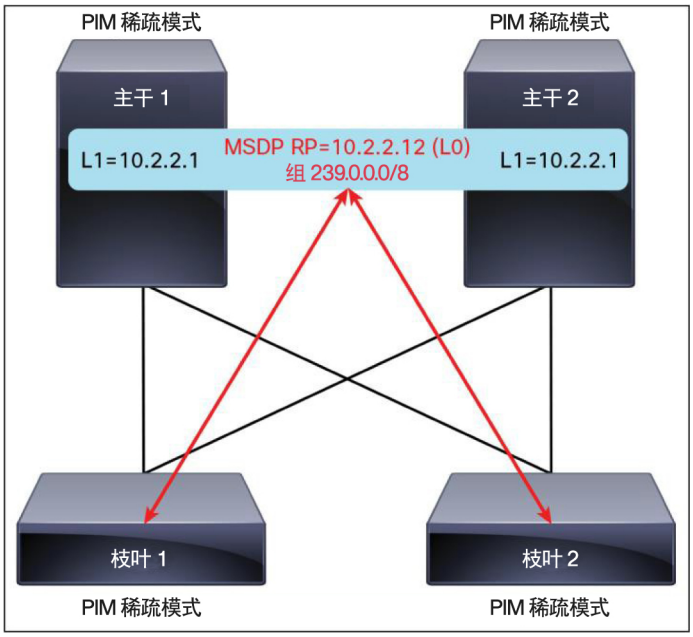


图 52. 枝叶组播配置

```
! Enable and configure PIM on the spine-facing interfaces

Leaf1(config)# feature pim
Leaf1(config)# interface Ethernet2/1-2
Leaf1(config)# ip pim sparse-mode

! Point to the RP address configured in the spines

Leaf1(config)# ip pim rp-address 10.2.2.12 group-list 239.0.0.0/8
```

在商业拓扑中使用 VXLAN

在商业设计，每个 VXLAN 网段可映射至应用或应用的相关层，例如网络层、应用层和数据库层。VXLAN 是一项可选功能，它是 Cisco Nexus 9000 系列交换机的许多独特优势之一。VXLAN 在 Cisco Nexus 9000 交换机上不是必需的；此处显示它只是为了强调它在商业设计中的可能用途和配置。

在此设计中，VXLAN 是为 VLAN 70、80 和 90 配置的，用于创建隧道以通过看起来很像第 2 层交换的方式进行分支间通信，尽管会路由底层基础设施。例如，通过为 vMotion VLAN 70 创建 VXLAN 网段，可在连接至支持 VXLAN 的分支的任何服务器间无中断地迁移虚拟机。随着基础设施的增长和分支的增加，此优势变得愈发重要，它允许虚拟机在数据中心中的任何位置迁移而不必担心 SPT 范围。

在分支交换机上配置 VXLAN。不必在此拓扑的主干交换机上配置 VXLAN。分支同时充当 VXLAN 隧道的源终端和目标终端，并充当网关以在隧道入口将 VLAN 网段转换为 VXLAN 网段，并在隧道出口将 VXLAN 转换回 VLAN 网段。服务器和设备永远不会看到 VXLAN 标记。主干必须支持分支上配置的组范围的组播路由。

配置 VXLAN 需要执行几个步骤：

- 启用 VXLAN 功能。
- 创建 /32 IP 并将其分配给专用环回接口。
- 通过传输路由协议来通告环回接口 /32 地址。
- 创建 VXLAN NVE 接口并将其附加至环回接口。
- 将 VXLAN 网段映射至组播组。
- 将 VLAN 映射至 VXLAN 网段。

在同样属于思科 vPC 域中的交换机上配置 VXLAN 时，还需要其他配置。在两台思科 vPC 对等交换机上，必须对连接至 NVE 接口的环回分配相同的备用 IP 地址。两台思科 vPC 对等交换机上的主要 IP 地址应该不同。

图 53 说明 VXLAN 配置。图 53 中提供了经过实验室测试的拓扑中的分支交换机的 VXLAN 配置示例。以类似方式配置另一台枝叶交换机。

图 53. VXLAN 设置

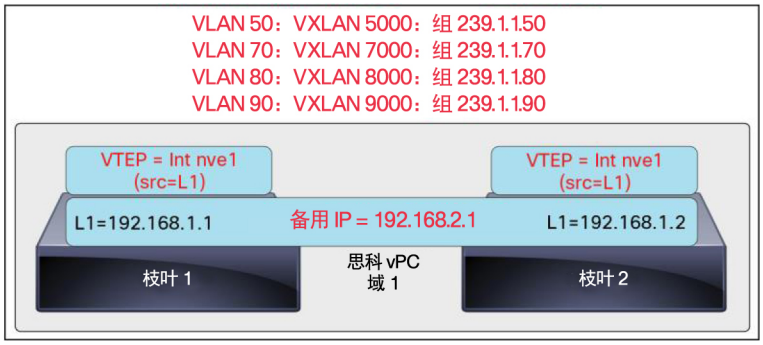


图 54. VXLAN 配置

```
! Enable VXLAN features

Leaf1(config)# feature nv overlay
Leaf1(config)# feature vn-segment-vlan-based

! Configure loopback used for VXLAN tunnels
! Configure secondary IP address for vPC support

Leaf1(config)# interface loopback1
Leaf1(config-if)# ip address 192.168.1.1/32
Leaf1(config-if)# ip address 192.168.2.1/32 secondary
Leaf1(config-if)# ip router eigrp 1
Leaf1(config-if)# ip pim sparse-mode

! Create NVE interface, using loopback as the source
! Bind VXLAN segments to an ASM multicast group

Leaf1(config-if)# interface nve1
Leaf1(config-if)# source-interface loopback1
Leaf1(config-if)# member vni 5000 mcast-group 239.1.1.50
Leaf1(config-if)# member vni 7000 mcast-group 239.1.1.70
Leaf1(config-if)# member vni 8000 mcast-group 239.1.1.80
Leaf1(config-if)# member vni 9000 mcast-group 239.1.1.90
Leaf1(config-if)# no shutdown
```

```
! Map VLANs to VXLAN segments

Leaf1(config-if)# vlan 50
Leaf1(config-vlan)# vn-segment 5000
Leaf1(config-vlan)# vlan 70
Leaf1(config-vlan)# vn-segment 7000
Leaf1(config-vlan)# vlan 80
Leaf1(config-vlan)# vn-segment 8000
Leaf1(config-vlan)# vlan 90
Leaf1(config-vlan)# vn-segment 9000
```

有关更多信息，请参阅“Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 6.0”（Cisco Nexus 9000 系列 NX-OS VXLAN 配置指南 6.0 版）的 Configuring vPCs（配置 vPC）一章。

服务设计和配置

正如之前讨论的，根据现有基础设施和流量模式，第 4-7 层服务设备可连接至 Cisco Nexus 9300 或 9500 交换机。在设计示例中，思科 ASA 5510 防火墙设备双宿至一对 Cisco Nexus 9300 交换机。

任意数目的不同供应商设备或服务设备可连接至一个 Nexus 9000 商业设计。在此拓扑中，DMZ 中有一些虚拟机，数据中心网络内部和外部有一些服务器。DMZ 是 VLAN 50，内部服务器在 VLAN 80 中，外部服务器和用户在 VLAN 90 中。Web 服务器的默认网关运行预思科 ASA 5510 防火墙设备上。防火墙接口针对每种流量划分为若干子接口，并具有关联至该子接口的正确 VLAN。此外，还有一个访问列表，用于指示哪些区域和设备可以相互通信。

图 55 中显示了经过实验室测试的设备中的思科 ASA 配置示例。未显示默认和/或无关的 ASA 配置。配置示例中使用了 ASA 8.4(7) 版。

图 55. 示例：思科 ASA 配置

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config)# no nameif
ciscoasa(config)# no security-level
ciscoasa(config)# no ip address

! Create DMZ subinterface, using VLAN 50
! Assign security level 50 to DMZ
! Assign an IP address to act as a gateway for VLAN 50

ciscoasa(config)# interface Ethernet0/0.50
ciscoasa(config)# description DMZ
ciscoasa(config)# vlan 50
ciscoasa(config)# nameif DMZ
ciscoasa(config)# security-level 50
ciscoasa(config)# ip address 10.1.50.254 255.255.255.0
```

```
! Create internal subinterface, using VLAN 80
! Assign security level 100 to internal zone
! Assign an IP address to act as a gateway for VLAN 80

ciscoasa(config)# interface Ethernet0/0.80
ciscoasa(config)# description internal
ciscoasa(config)# vlan 80
ciscoasa(config)# nameif inside
ciscoasa(config)# security-level 100
ciscoasa(config)# ip address 10.1.80.254 255.255.255.0

! Create DMZ subinterface, using VLAN 90
! Assign security level zero to outside zone

ciscoasa(config)# interface Ethernet0/0.90
ciscoasa(config)# description outside
ciscoasa(config)# vlan 90
ciscoasa(config)# nameif outside
ciscoasa(config)# security-level 0
ciscoasa(config)# no ip address

! Create object to include DMZ subnet 10.1.50.0/24

ciscoasa(config)# object network DMZ
ciscoasa(config)# subnet 10.1.50.0 255.255.255.0

! Create object group to match web and HTTP traffic

ciscoasa(config)# object-group service WEB
ciscoasa(config)# service-object tcp destination eq www
ciscoasa(config)# service-object tcp destination eq https

! Create access list to permit DMZ 10.1.50.0/24 web and
! HTTP traffic

ciscoasa(config)# access-list 101 extended permit object-group WEB any object DMZ

! Apply access list to ingress traffic on the outside
! interface

ciscoasa(config)# access-group 101 in interface outside
```

有关思科 ASA 解决方案的更多信息，请参阅[思科 ASA 5500-X 系列下一代防火墙网页](#)。

交换矩阵管理和自动化

Cisco UCS Director

Cisco UCS Director 是一个非常强大的集中管理和协调工具，它可以让小型商业公司 IT 员工的日常操作变得非常轻松。通过 Cisco UCS Director 提供的自动化功能，少量 IT 员工即可加速交付新服务和应用。Cisco UCS Director 将硬件和软件抽象化为可编程任务，并使用工作流程设计器以允许系统管理员将任务拖放到工作流程中以提供必要的资源。图 56 描绘了 Cisco UCS Director 工作流程示例。

图 56. 示例：Cisco UCS Director 工作流程

Cisco UCS Director 允许您将通常从思科 UCS 管理器 GUI 手动执行的许多常见任务自动化。下表列出了可借助 Cisco UCS Director 实现自动化的许多任务。

表 3. 常见的 UCS Director 自动化任务

1. 选择 UCS 服务器	21. 修改 UCS 引导策略 WWPN
2. 创建 UCS 服务器池	22. 创建 VLAN 组
3. 删除 UCS 服务器池	23. 删除 UCS VLAN 组
4. 将服务器添加到 UCS 服务器池	24. 修改 UCS VLAN/VLAN 组组织权限
5. 从 UCS 服务器池中删除服务器	25. 服务器维护
6. 关联 UCS 服务配置文件模板	26. 重新确认服务器插槽
7. 重置 UCS 服务器	27. 添加 VLAN
8. 打开 UCS 服务器电源	28. 删除 UCS 引导策略
9. 关闭 UCS 服务器电源	29. 删除 UCS VLAN
10. 通过模板创建 UCS 服务配置文件	30. 将 VLAN 添加到服务配置文件
11. 创建 UCS 服务配置文件	31. 从服务配置文件中删除 VLAN
12. 选择 UCS 服务配置文件	32. 从服务配置文件中添加 iSCSI vNIC
13. 修改 UCS 服务配置文件引导策略	33. 从服务配置文件中删除 ISCSI vNIC
14. 删除 UCS 服务配置文件	34. 从服务配置文件中添加 vNIC
15. 关联 UCS 服务配置文件	35. 从服务配置文件中删除 vNIC
16. 取消 UCS 服务器关联	36. 创建服务配置文件 iSCSI 引导策略
17. 取消关联 UCS 服务配置文件	37. 将服务配置文件引导策略修改为从 iSCSI 引导
18. 创建 UCS 引导策略	38. 从服务配置文件 vNIC 中删除 VLAN
19. 修改 UCS 引导策略 LUN ID	39. 将 VLAN 添加到 vNIC 模板
20. 克隆 UCS 引导策略	40. 从 vNIC 模板中删除 VLAN

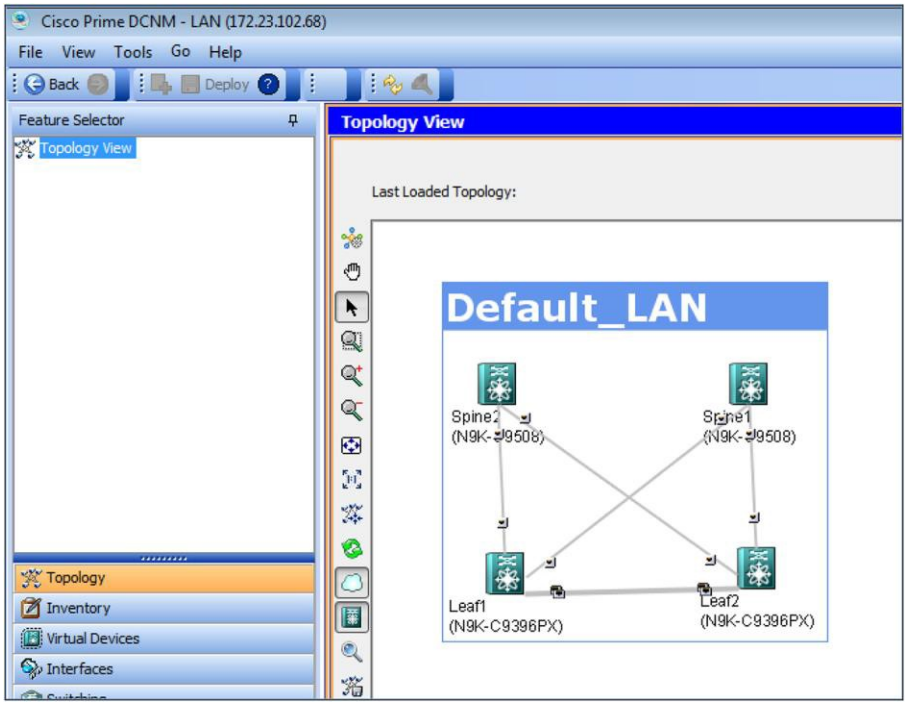
有关更多信息，请参阅思科 UCS Director 解决方案概述。

Cisco Prime 数据中心网络管理器

Cisco Prime™ 数据中心网络管理器 (DCNM) 是一个非常强大的工具，用于思科数据中心计算、网络和存储基础设施的集中数据中心监控、管理和自动化。Cisco Prime DCNM 基本版本免费提供。更高级的功能需要许可证。Cisco Prime DCNM 允许集中管理所有 Cisco Nexus 交换机以及思科 UCS 和 MDS 设备。

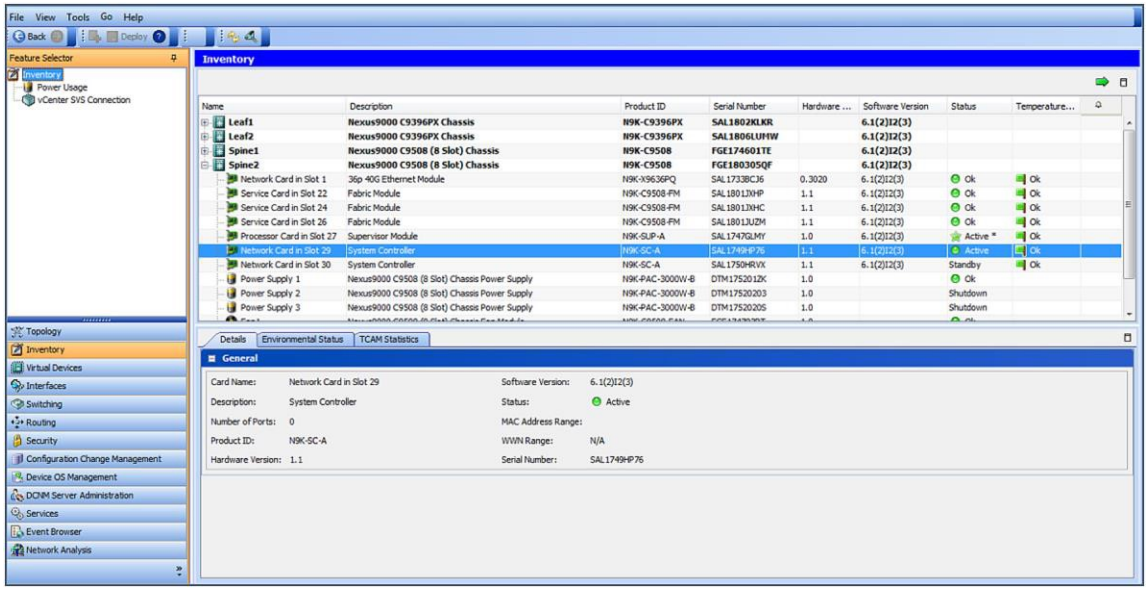
基础设施管理的设计示例中使用了 Cisco Prime DCNM LAN 6.0 版。Cisco Prime DCNM 的一项强大功能是能够具有可视的自动更新拓扑图。下图描绘了实验室拓扑示例。

图 57. Cisco Prime DCNM 拓扑图



Cisco Prime DCNM 还可用于管理高级功能，例如，思科虚拟 PortChannel (vPC)、NX-OS 映像管理和资产控制。图 58 显示了其中一台主干交换机中的虚拟资产示例。

图 58. Cisco Prime DCNM 交换机资产



总结

Cisco Nexus 9000 系列交换机是一款经济实惠且功能强大的交换机，可轻松用于中小型商业数据中心。随着您的应用增长，包含两台交换机的部署提供一种通过经济实惠的光纤从 1 GB 到 10 GB 到 40 GB 的路径，该部署具有能够提供冗余性的丰富功能集，允许使用所有链路，执行等价多路径，并且具有可选重叠，具体视应用的需求而定。Cisco Nexus 9000 系列交换机还可与快要过时的环境轻松集成，以避免您更换现有的基础设施。

附录 A：自动化和可编程性

下面是有关自动化工具（包括 Puppet）的信息。

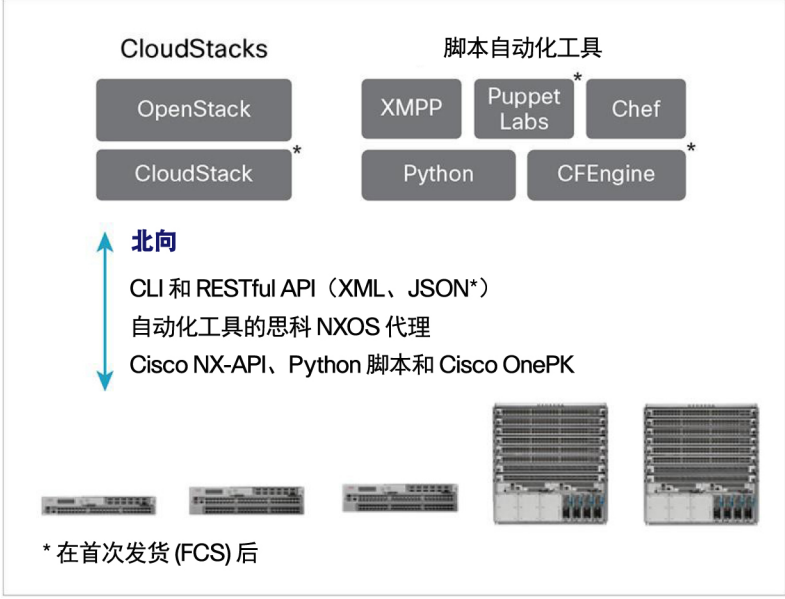
自动化工具

将新应用部署至网络时，需要调配基础设施资源以启用这些应用。从网络角度而言，可能需要自动化各种配置任务，例如 VLAN 和 VXLAN 调配、QoS 以及添加新路由。随着应用的增长和变化，可能还需要更改网络配置以允许或限制各层之间的通信或根据应用需要调整网络。

网络设备需要提供全面的自动化功能和 API 以支持新的配置更改和运营模型。Cisco Nexus 9000 交换机上的增强型 Cisco NX-OS 与多个开放源和商业生态系统合作伙伴集成，以实现自动化、协调、可编程性、监控及合规性支持。

除了 Cisco NX-OS 命令行接口外，Cisco Nexus 9000 交换机还提供了多个北向 API 以展示 CLI 上可用的所有功能，并为使用强大的自动化功能提供方便。图 59 显示了支持的自动化工具。

图 59. Cisco Nexus 9000 API 集成

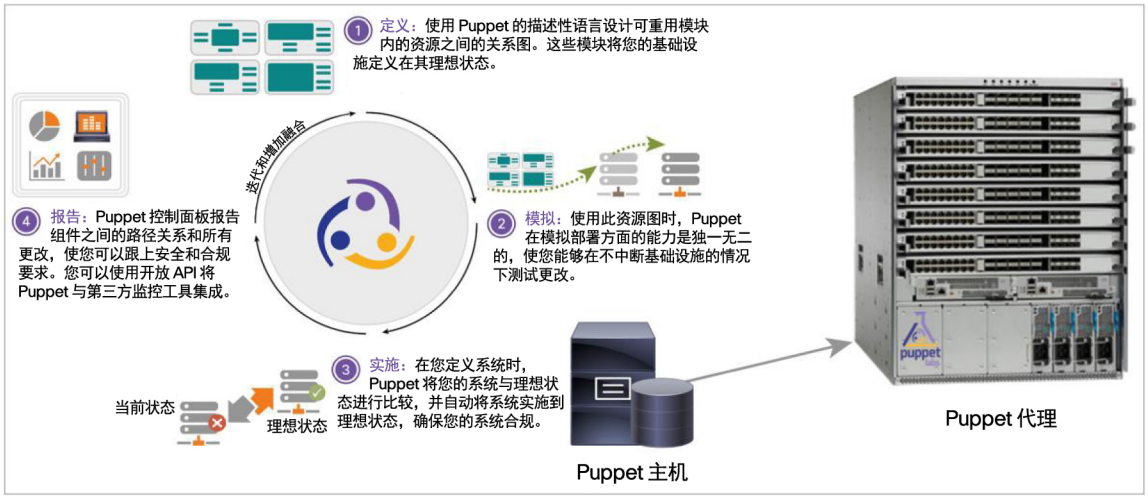


通过 Puppet 实现自动化

Puppet 是 Cisco Nexus 9000 系列交换机上用于实现自动化的多个工具选项之一，但它在本解决方案指南中用作主要示例。Puppet 是一款自动化软件，它允许系统管理员通过描述强制 Puppet 代理中运行的设备状态保持一致且可复用的风格，从而减少所需的手动配置量或一次性脚本量。Puppet 在 DevOps 社区中已广泛部署且备受好评。

Puppet 使用描述性语言，这意味着管理员告诉 Puppet 他们所希望的最终结果或配置，而非告诉有关完成方式的详细信息。如果 Cisco Nexus 9000 交换机上安装了 Puppet 代理，那么管理员告诉 Puppet 他的意图（一组可重用的配置或管理任务，称为清单），然后该清单部署至 Nexus 9000 并转换为 NX-OS 配置。图 60 中提供了 Cisco Nexus 9000 系列交换机和 Puppet 集成的概述。

图 60. Puppet 工作流程概述



有用的链接

本部分提供了本白皮书中包括的所有链接的完整列表，以及其他有用的参考资料。

思科 ACI 模式

- ACI 主页：思科以应用为中心的基础设施

外部资源

- Cisco OpenStack
- Puppet 是什么？

一般指南

- 所有 Nexus 9000 配置指南
- Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches, Release 6.0（Cisco Nexus 9000 系列交换机的 Cisco Nexus 2000 系列 NX-OS 交换矩阵扩展器配置指南 6.0 版）
- Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS 接口配置指南 6.0 版）
- Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS 服务质量配置指南 6.0 版）

- Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS 系统管理配置指南 6.0 版）
- Cisco Nexus 9000 Series Switches Compare Models tool（Cisco Nexus 9000 系列交换机型号对比工具）
- Cisco Nexus 9500 Series Switches Architecture（Cisco Nexus 9500 系列交换机架构）
- Configuring Cisco vPCs on Cisco Nexus 9000 NX-OS（在 Cisco Nexus 9000 NX-OS 上配置思科 vPC）
- MIBs Supported from Cisco NX-OS Release 6.1(2)I2（从 Cisco NX-OS Release 6.1(2)I2 开始支持的 MIB）
- Migrate from Cisco Catalyst 6500 Series Switches to Cisco Nexus 9000 Series Switches（从 Cisco Catalyst 6500 系列交换机迁移到 Cisco Nexus 9000 系列交换机）
- Cisco vPC Best Practices Design Guide（思科 vPC 最佳实践设计指南）

许可

- Licensing Cisco NX-OS Software Features（许可 Cisco NX-OS 软件功能）

Cisco Nexus 9000 产品手册

- 所有 Cisco Nexus 9000 产品手册
- Cisco Nexus 9500 Platform Switches Data Sheet（Cisco Nexus 9500 平台交换机产品手册）
- Cisco Nexus 9300 Platform Switches Data Sheet（Cisco Nexus 9300 平台交换机产品手册）
- Cisco Nexus 9500 and 9300 Series Switches NX-OS Software Data Sheet（Cisco Nexus 9500 和 9300 系列交换机 NX-OS 软件产品手册）

其他思科产品

- 思科 ASA 5500-X 系列下一代防火墙
- Cisco Nexus 5600 Platform Switches Data Sheet（Cisco Nexus 5600 平台交换机产品手册）
- Cisco UCS Director 解决方案概述
- Cisco Unified Computing System Express
- 存储网络网页

其他重叠和协议

- BGP MPLS Based Ethernet VPN IETF Draft（基于 BGP MPLS 的以太网 VPN IETF 草案）
- Cisco FabricPath 网页
- Cisco Locator/ID Separation Protocol (LISP) 网页
- Cisco NX-OS/IOS 比较
- Cisco Overlay Transport Virtualization Technology Introduction and Deployment Considerations（思科重叠传输虚拟化技术简介和部署注意事项）
- Data Center Overlay Technologies white paper（数据中心重叠技术白皮书）
- Cisco Nexus 7000 FabricPath 白皮书
- 重叠传输虚拟化网页

软件版本说明

- 所有 Cisco Nexus 9000 版本说明
- Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS 软件升级和降级指南 6.0 版）
- Cisco NX-OS Version 6.1(2)I2(3) release notes（Cisco NX-OS 版本 6.1(2)I2(3) 版本说明）

收发器

- Cisco 10GBase SFP Modules data sheet（Cisco 10GBase SFP 模块产品手册）
- Cisco Transceiver Modules compatibility information（思科收发器模块兼容性信息）
- Cisco QSA data sheet（Cisco QSA 产品手册）
- Cisco QSFP BiDi Technology white paper（Cisco QSFP BiDi 技术白皮书）

单播和组播路由

- Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS 组播路由配置指南 6.0 版）
- Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS 单播路由配置指南 6.0 版）
- Configuring MSDP（配置 MSDP）
- Configuring PIM（配置 PIM）

VXLAN

- Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 6.0（Cisco Nexus 9000 系列 NX-OS VXLAN 配置指南 6.0 版）
- Configuring VXLAN（配置 VXLAN）
- VXLAN Overview: Cisco Nexus 9000 Series Switches（VXLAN 概述：Cisco Nexus 9000 系列交换机）

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。

美国印刷

C07-733228-00 11/14