软件定义接入

解决方案设计指南

2019 年 10 月

目录

思科全数字化网络架构和软件定义接入

思科® 软件定义接入 (SD-Access) 从传统园区 LAN 设计演变而来，是一种可直接实施组织意图的网络解决方案。SD-Access 通过作为 Cisco DNA Center 软件一部分运行的应用程序包启用，该软件用于设计、调配和应用策略，并通过网络状态感知使智能园区有线和无线网络的创建变得更加便捷。

*交换矩阵技术*是 SD-Access 不可或缺的一部分，可以为有线和无线园区网络提供可编程的重叠网络和易于部署的网络虚拟化，从而允许物理网络根据需要托管一个或多个逻辑网络以满足设计意图。除网络虚拟化以外，园区网络交换矩阵技术还可以增强通信控制，根据用户身份和组成员身份进行软件定义的分段和策略实施。软件定义的分段借助思科 TrustSec® 技术实现无缝集成，通过在虚拟网络内使用可扩展组标记 (SGT) 来为可扩展组提供微分段功能。使用 Cisco DNA Center 自动创建虚拟网络可减少运营支出，同时还可提供以下优势：通过集成的安全功能降低风险；通过网络状态感知和分析功能提高网络性能。

本设计指南首先概述有助于推动园区网络设计发展的各项要求，然后介绍可用于构建 SD-Access 网络以满足这些要求的最新技术和设计。本指南是 SD-Access 相关部署指南的配套文档，这些部署指南提供了相关配置，并说明如何部署本指南所述设计的最常见的实施。本指南的目标读者是具有以下需求的技术决策者：希望了解思科园区产品和可用技术选项，以及用于设计出最符合组织需求的网络的领先实践。

配套资源

有关配套的《软件定义接入和 Cisco DNA Center 管理基础设施规范化部署指南》、《软件定义接入大中型站点交换矩阵调配规范化部署指南》、《用于分布式园区的软件定义接入规范化部署指南》、相关部署指南、设计指南和白皮书，请访问以下页面：

- https://www.cisco.com/go/designzone
- https://cs.co/en-cvds

如果您不是从思科社区或设计区下载的本指南，可查看本指南的最新版本。

扩展指标和延迟信息

有关扩展指标和延迟信息，请参阅思科社区中的 SD-Access 资源和延迟设计指南。

全数字化组织的网络要求

随着全数字化的发展，在某些情况下，软件应用正在从单纯地支持业务流程演变成为主要的企业收入来源和竞争优势。当今组织无时无刻不面临着挑战，他们需要扩展网络容量以迅速应对应用需求和增长。因为园区局域网是位于某个位置的用户和设备用于访问应用的网络，所以应该增强园区有线和无线局域网功能以支持上述不断变化的需求。

以下是驱动现有园区网络发展的关键要求。

为增长和扩展提供灵活的以太网基础

- **简化部署和自动化** - 使用开放式 API 通过集中式控制器配置和管理网络设备，极快地部署网络设备和服务，同时降低部署风险。
- **增加带宽需求** - 在一个网络的整个生命周期内，带宽需求会翻上一倍甚至多倍，这导致新的网络需要具备汇聚的能力，随着时间的推移，使用的容量可以从 10 Gbps 以太网增加到 40 Gbps、100 Gbps。
- **提高无线接入点的容量** - 对采用最新第二代 802.11ac 技术的无线接入点 (AP) 的带宽需求现在已超过 1 Gbps，并且 IEEE 现已批准定义 2.5 Gbps 和 5 Gbps 以太网的 802.3bz 标准。思科 Catalyst® 多千兆技术无需升级现有铜缆以太网布线即可支持该带宽需求。

- **以太网设备提出了额外的功率要求** – 照明设备、监控摄像头、虚拟桌面终端、远程接入交换机和 AP 等新设备可能需要更高的功率才能工作。接入层的设计应该能够支持每端口 60W 的以太网供电（通过思科通用型以太网供电技术提供），而且接入层还应该在交换机升级和重新启动事件期间提供以太网供电 (PoE) 永久电源。思科 Catalyst 9000 系列接入层交换机支持永久 PoE，且其硬件能够支持未来将会面市的每端口 100W 技术。

集成的服务和安全性

- **一致的有线和无线安全功能** – 无论用户连接到有线以太网端口还是通过无线局域网连接，下述安全功能都应该保持一致。
- **网络状态感知和分析** – 利用遥测提高网络、设备和应用的性能，从而主动预测与网络和安全相关的风险，甚至包括加密流量中存在的风险。
- **身份服务** – 通过对组成员身份使用 STG 并将设备映射到虚拟网络 (VN) 中，标识连接到网络的用户和设备的身份可提供实施安全策略以进行访问控制和网络分段所需的的情景信息。
- **基于组的策略** – 根据用户组信息创建访问和应用策略，可提供更加简单且可扩展的安全策略部署和管理方式。传统的访问控制列表 (ACL) 可能难以实施、管理和扩展，因为它们依靠 IP 地址和子网等网络结构。
- **软件定义的分段** – 从基于组的策略中分配的可扩展组标记可用于对网络进行分段，以便在物理和虚拟网络中实现数据平面隔离。
- **网络虚拟化** – 能够在共享一个通用基础设施的同时支持数据平面和控制平面相互隔离的多个虚拟网络，从而安全地隔离不同的用户组和应用组。

用于医疗网络的 SD-Access 使用案例：安全分段和分析

对于攻击者来说，我们的医疗记录与信用卡号和在线密码一样有价值。随着最近网络攻击的发生，医院需要具有符合 HIPAA 标准的有线和无线网络，以便全面持续地洞察他们的网络流量，从而保护敏感的医疗设备（例如电子病历服务器、生命体征监测仪或护士工作站），使恶意设备不会危及网络。

患者的移动设备感染恶意软件后会改变网络通信行为，以传播恶意软件并感染其他终端。如果患者的移动设备与任何医疗设备进行通信，会被视为异常行为。SD-Access 可以通过使用宏分段并将设备置于不同的重叠网络中实现隔离，从而满足完全隔离患者设备和医疗机构设备的需求。

在类似的场景中，如果遭到感染的是医疗专业人员的移动设备，而这些设备需要连接信息系统以执行某些任务，但无需连接其他医疗设备，如何处理这种情况？SD-Access 可在设备和用户进入网络时对其进行分析并在重叠网络中应用微分段来满足这一分段需求，而不只是简单地进行网络隔离。通过灵活地创建策略，可对设备类型和用户角色进行分组，从而将通信限制在组内，或者仅在实施组织策略的意图需要时才启用组之间的通信。

借助 Cisco DNA Center 内置的自动化功能，可简化部署预期结果以满足组织需求的过程，且这些简化同时适用于有线域和无线域。

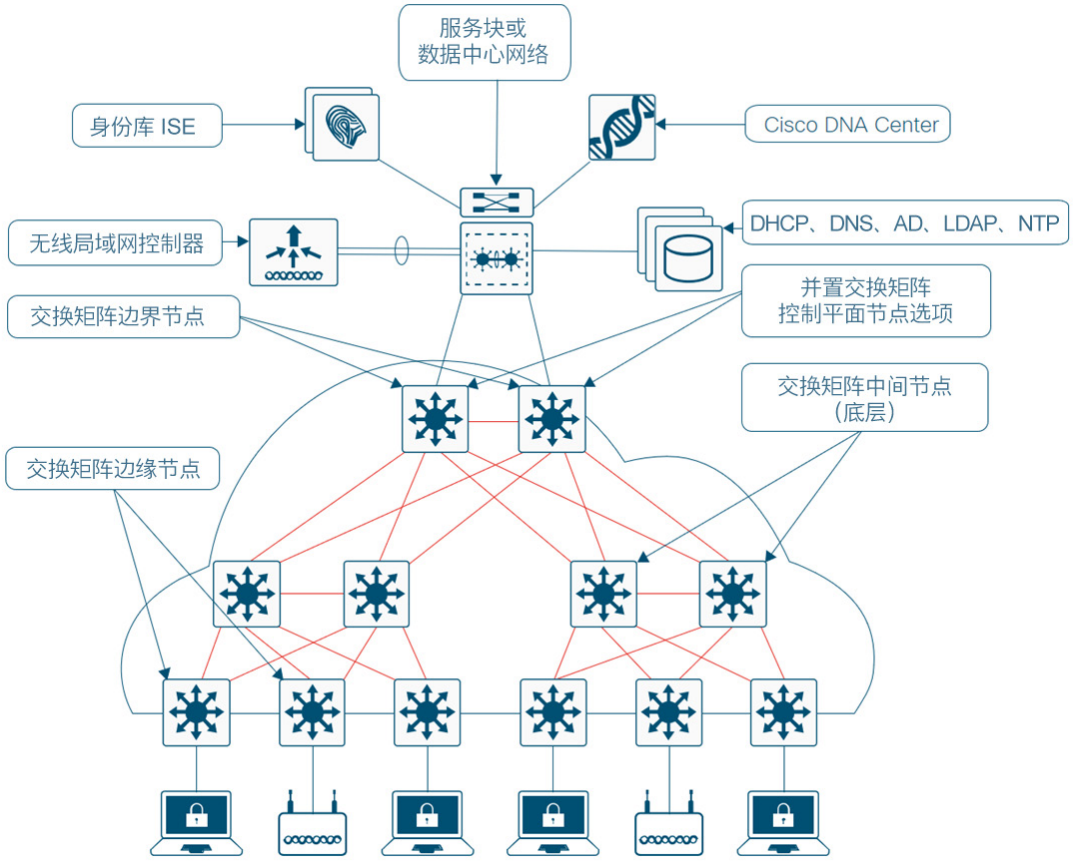
其他组织可能拥有与医疗机构类似的业务要求，也需要进行安全的分段和分析：

- **教育业** – 大学校园分为行政网络和学生宿舍网络。
- **零售业** – 隔离销售终端机，支持实现支付卡行业合规性。
- **制造业** – 隔离制造车间的机器间流量。
- **医疗业** – 将网络专用于医疗设备、患者无线访客接入和 HIPAA 合规性方面。
- **企业** – 并购期间的网络集成，在此情况下可能存在重叠的地址空间；隔离楼宇控制系统和视频监控设备。

SD-Access 解决方案组件

SD-Access 解决方案将 Cisco DNA Center 软件、身份服务及有线和无线交换矩阵功能完美结合。在 SD-Access 解决方案中，交换矩阵站点由一组独立的交换矩阵控制平面节点、边缘节点、中间（仅传输）节点和边界节点组成。无线集成使交换矩阵站点可以增加交换矩阵 WLC 和交换矩阵模式 AP 组件。交换矩阵站点可以使用不同类型的传输网络（如 IP 传输网络、SD-WAN 传输网络 [未来] 和 SD-Access 传输网络）进行互连，以建立更大的交换矩阵域。此部分介绍每个角色的功能、各角色在物理园区拓扑中的对应角色，以及解决方案管理、无线集成和策略应用所需的组件。

图 1. SD-Access 解决方案和交换矩阵组件



控制平面节点

SD-Access 交换矩阵控制平面节点基于合并到同一个节点上的 LISP 映射服务器 (MS) 和映射解析器 (MR) 功能。控制平面数据库跟踪交换矩阵站点中的所有终端并将这些终端关联到交换矩阵节点，从而分离终端 IP 地址或 MAC 地址与网络中的位置（距离最近的路由器）。控制平面节点功能可以与边界节点搭配使用，也可以利用专用节点进行扩展，并使用两到六个节点（仅适用于有线部署）实现恢复能力。边界和边缘节点向所有控制平面节点注册并使用所有控制平面节点，因此选定的弹性节点应为相同类型，从而确保性能一致。

控制平面节点可实现以下功能：

- **主机跟踪数据库** - 主机跟踪数据库 (HTDB) 是存储 EID 与交换矩阵边缘节点绑定关系的中央存储库。
- **映射服务器** - LISP MS 用于通过来自交换矩阵边缘设备的注册消息填充 HTDB。
- **映射解析器** - LISP MR 用于响应交换矩阵边缘设备请求目的 EID 的 RLOC 映射信息的映射查询。

边缘节点

SD-Access 交换矩阵边缘节点相当于传统园区 LAN 设计中的接入层交换机。边缘节点实施第 3 层接入设计，外加以下交换矩阵功能：

- **终端注册** - 每个边缘节点都有一个面向所有控制平面节点的 LISP 控制平面会话。交换矩阵边缘检测到终端后，会将其添加到本地主机跟踪数据库（称为 EID 表）。边缘设备还会发出 LISP 映射注册消息，向控制平面节点通知检测到的终端，以便其填充 HTDB。
- **将用户映射到虚拟网络** - 通过将终端分配到与 LISP 实例关联的 VLAN 和交换机虚拟接口 (SVI)，可将终端放入虚拟网络。可以使用 802.1X，以静态或动态方式将终端映射到 VLAN 中。系统还分配 SGT，SGT 可用于在交换矩阵边缘提供分段和策略实施。

技术提示
Cisco IOS® 软件使用思科基于身份的网络服务 (IBNS) 2.0 增强 802.1X 设备的功能。例如，添加了并发身份验证方法和接口模板。同样，Cisco DNA Center 也得到了增强，以帮助完成从 IBNS 1.0 到 2.0 配置的过渡，这些配置使用思科通用分类策略语言（通常称为 C3PL）。有关其他配置功能，请参阅版本说明和更新的部署指南。有关 IBNS 的更多信息，请参阅：https://cisco.com/go/ibns。

- **任播第 3 层网关** - 可以在一个通用 EID 子网中的每个节点上使用通用网关（IP 和 MAC 地址），从而实现跨不同 RLOC 的最佳转发和移动性。
- **LISP 转发** - 交换矩阵边缘节点使用的不是基于路由的常用决策，而是通过查询映射服务器来确定与目的 EID 关联的 RLOC，并将该信息作为流量目的地信息。如果无法解析目的 RLOC，该节点会将流量发送到默认的交换矩阵边界，在其中使用全局路由表进行转发。从映射服务器收到的响应存储于 LISP 映射缓存中，后者被合并到思科快速转发表并安装到硬件中。如果在交换矩阵边缘收到流向非本地连接终端的流量，则会向发送方交换矩阵边缘发送 LISP 查询映射请求，以便触发新的映射请求；这可以应对终端位于不同交换矩阵边缘交换机上的情况。
- **VXLAN 封装/解封** - 交换矩阵边缘节点使用与目的 IP 地址关联的 RLOC 来封装具有 VXLAN 报头的流量，并以类似方式解封在目的 RLOC 上接收的 VXLAN 流量。通过对流量进行封装和解封，可以更改终端位置并使用网络中的其他边缘节点和 RLOC 对终端位置进行封装，而无需在封装中更改终端地址。

中间节点

交换矩阵中间节点是第 3 层网络的一部分，用于边缘节点与边界节点之间的互联。在使用核心层、分布层和接入层的三层园区设计中，中间节点相当于分布层交换机，但中间节点的数量不限于单层设备。中间节点在交换矩阵内部路由和传输 IP 流量。对于中间节点，没有 VXLAN 封装/解封、LISP 控制平面消息或 SGT 感知方面的要求，只有一个额外的交换矩阵 MTU 要求，即能够承受封装了 VXLAN 信息的更大 IP 数据包。

边界节点

交换矩阵边界节点用作 SD-Access 交换矩阵站点和交换矩阵外部网络之间的网关。交换矩阵边界节点负责网络虚拟化互通，以及从交换矩阵到网络其余部分的 SGT 传播。大多数网络使用外部边界作为交换矩阵的通用出口点，例如用于企业网络的其余部分以及互联网。外部边界是为交换矩阵中的所有虚拟网络提供默认出口点的高效机制，无需导入任何外部路由。交换矩阵边界节点可选择配置为内部边界，作为特定网络地址（例如共享服务或数据中心网络）的网关运行，其中外部网络在交换矩阵中虚拟网络的显式出口点导入到这些虚拟网络中。边界节点还可具有组合角色，充当任意位置边界（包括内部边界和外部边界），这在具有边界要求但仅靠外部边界无法满足要求的网络中很有用，在此类网络中，其中一个外部边界也是需要使用内部边界功能来导入特定路由的一个位置。

边界节点实施以下功能：

- **通告 EID 子网** - SD-Access 将边界网关协议 (BGP) 配置为首选路由协议，用于通告交换矩阵外部的 EID 前缀和从交换矩阵外部经边界节点传入 EID 子网的流量。这些 EID 前缀只出现在边界上的路由表中，而在交换矩阵的其余各处，则使用交换矩阵控制平面来访问 EID 信息。
- **交换矩阵域出口点** - 外部交换矩阵边界是交换矩阵边缘节点的最后选用网关。此出口点使用 LISP 代理隧道路由器功能实施。此出口点也可以是连接到网络的内部交换矩阵边界，有一组明确定义的 IP 子网，这增加了在交换矩阵中通告这些子网的要求。
- **将 LISP 实例映射到 VRF** - 交换矩阵边界可以使用外部 VRF 实例和 VRF 感知路由协议将网络虚拟化从交换矩阵内部扩展到交换矩阵外部，以保留虚拟化。
- **策略映射** - 交换矩阵边界节点还可以从交换矩阵内部映射要在退出该交换矩阵时适当维护的 SGT 信息。通过使用 SGT 交换协议 (SXP) 将标记传输到思科 TrustSec 感知设备，或通过为连接到边界节点而实施的内联标记功能直接将 SGT 映射到数据包中的思科元数据字段，可以将 SGT 信息从交换矩阵边界节点传播到交换矩阵外部的网络。

扩展节点

通过将思科工业以太网交换机连接到思科 Catalyst 9000 系列 SD-Access 交换矩阵边缘节点，您可以将交换矩阵功能扩展到思科工业以太网交换机（例如思科 Catalyst 数字化楼宇系列和工业以太网 3000、4000 和 5000 系列），从而实现用户终端和 IoT 设备的分段。

借助 Cisco DNA Center 自动化功能，充当扩展节点角色的交换机可以使用 802.1Q 中继通过具有一个或多个物理成员的 EtherChannel 连接到交换矩阵边缘，并通过零接触即插即用功能被发现。终端（包括交换矩阵模式 AP）连接到扩展节点交换机。交换矩阵调配过程中，通过主机自行激活分配 VLAN 和 SGT。可扩展组标记策略在交换矩阵边缘实施。

使用扩展节点来扩展交换矩阵功能的好处在于，可借助基于 Cisco DNA Center 的自动化功能简化物联网运营，跨 IT 和 OT 实施一致策略，并且提高对物联网设备的网络可视性。

有关扩展节点的更多信息，请访问：https://www.cisco.com/go/iot。

交换矩阵无线局域网控制器

交换矩阵 WLC 与交换矩阵控制平面集成。交换矩阵 WLC 和非交换矩阵 WLC 提供 AP 映像和配置管理、客户端会话管理及移动服务。通过在无线客户端加入事件期间将无线客户端的 MAC 地址注册到交换矩阵控制平面的主机跟踪数据库，以及在客户端漫游事件期间提供交换矩阵边缘 RLOC 位置更新，交换矩阵 WLC 还可为交换矩阵集成提供其他服务。

它与非交换矩阵 WLC 行为的主要区别在于，对于支持交换矩阵的 SSID，交换矩阵 WLC 并非主动参与数据平面流量转发，这些 SSID 通过交换矩阵模式 AP 直接将流量转发到交换矩阵边缘。

通常，交换矩阵 WLC 设备连接到交换矩阵和交换矩阵边界外部的共享服务分布层块或数据中心，这意味着其管理 IP 地址存在于全局路由表中。为使无线接入点建立用于 WLC 管理的 CAPWAP 隧道，无线接入点必须位于有权访问外部设备的 VN 中。在 SD-Access 解决方案中，Cisco DNA Center 将无线接入点配置为驻留在名为 INFRA_VRF 的 VRF 中，这将映射到全局路由表，从而确保无需路由渗透或融合路由器（选择性共享路由信息的多 VRF 路由器）服务即可建立连接。每个交换矩阵站点都必须具有对该站点而言唯一的 WLC。建议将 WLC 置于本地站点内，因为 SD-Access 对延迟有要求。下一部分将更详细地介绍延迟。

思科 SD-Access 中小型部署可以使用思科 Catalyst 9800 嵌入式无线控制器。该控制器可作为软件包更新用于 Catalyst 9300 交换机，为有线和无线（仅交换矩阵）基础设施提供一致的策略、分段、安全性及无缝移动性，同时保

持思科统一无线网络的易操作性。无线控制平面保持不变，使用在 AP 上启动以及在思科 Catalyst 9800 嵌入式无线控制器上终止的 CAPWAP 隧道。数据平面对 AP 和交换矩阵边缘之间的重叠网络流量使用 VXLAN 封装。

用于 Catalyst 9300 系列软件包的 Catalyst 9800 嵌入式无线控制器只能在采用以下两种受支持拓扑的思科 SD-Access 部署中实现无线功能:

- 思科 Catalyst 9300 系列交换机充当并置边界和控制平面。
- 思科 Catalyst 9300 系列交换机充当一体化交换矩阵。

嵌入式控制器仅支持交换矩阵模式无线接入点。

交换矩阵模式无线接入点

交换矩阵模式 AP 是与交换矩阵 WLC 关联的采用思科 WiFi6 (802.11ax) 以及第二代和第一代 802.11ac 技术的 AP，它已经配置有一个或多个支持交换矩阵的 SSID。交换矩阵模式 AP 将继续支持传统 AP 所支持的无线介质服务；应用 AVC、服务质量 (QoS) 和其他无线策略；并建立通往交换矩阵 WLC 的 CAPWAP 控制平面。交换矩阵无线接入点作为本地模式无线接入点加入，并且必须直接连接到交换矩阵边缘节点交换机才能启用交换矩阵注册事件，包括通过交换矩阵 WLC 分配 RLOC。交换矩阵边缘节点使用 CDP 将 AP 识别为特殊有线主机，应用特殊端口配置并将 AP 分配给交换矩阵的公用 EID 空间中唯一的重叠网络。通过使用单个子网覆盖交换矩阵站点的无线接入点基础设施，此分配可简化管理。

当无线客户端连接到交换矩阵模式无线接入点并经身份验证连接到支持交换矩阵的无线局域网中时，WLC 将使用客户端第 2 层 VNI 和 ISE 提供的 SGT 更新交换矩阵模式无线接入点。然后，WLC 充当出口交换矩阵边缘节点交换机的代理将无线客户端第 2 层 EID 注册到控制平面中。建立初始连接后，该无线接入点使用第 2 层 VNI 信息将以太网连接上的无线客户端通信通过 VXLAN 封装到直接连接的交换矩阵边缘交换机。交换矩阵边缘交换机将客户端流量映射到与该 VNI 关联的相应 VLAN 接口中以便在交换矩阵中进行转发，并向控制平面数据库注册无线客户端 IP 地址。

身份服务引擎

思科 ISE 是一种安全的网络接入平台，能够提高访问组织网络的用户和设备的管理感知性、可控性和一致性。ISE 是 SD-Access 实施策略时不可或缺的组成部分，可以将用户和设备动态映射到可扩展的组，并简化端到端安全策略实施。在 ISE 内，在简单而灵活的界面中显示用户和设备。通过在 ISE 上使用思科平台交换架构 (pxGrid) 和 REST API 交换客户端信息并自动完成与交换矩阵相关的配置，ISE 可与 Cisco DNA Center 集成。SD-Access 解决方案通过以下方式集成思科 TrustSec：对基于组的策略提供端到端支持，包括数据平面流量的 VXLAN 报头中的 SGT 信息，同时采用分配唯一 VNI 的方法支持多个 VN。组、策略、AAA 服务（身份验证、授权和记账）及终端分析由 ISE 驱动并通过 Cisco DNA Center 的策略制定工作流程进行协调。

可扩展的组以 SGT 进行标识，SGT 是 VXLAN 报头中传输的 16 位值。SGT 由思科 ISE 集中定义和管理。ISE 和 Cisco DNA Center 通过 REST API 紧密集成，策略的管理由 Cisco DNA Center 驱动。

ISE 支持独立式和分布式部署模型。此外，可以同时部署多个分布式节点，从而支持故障切换恢复能力。选项范围允许支持数十万个终端设备，其中用于 SD-Access 的设备的子集应遵循本指南下文介绍的限制。至少，建议将基本双节点 ISE 部署用于 SD-Access 部署，其中每个节点运行所有服务以实现冗余。

SD-Access 交换矩阵边缘节点交换机将身份验证请求发送到在 ISE 上运行的策略服务节点 (PSN) 角色。在独立部署的情况下，具有或不具有节点冗余的 PSN 角色由单个 IP 地址引用。ISE 分布式模型使用多个活动 PSN 角色，其中每个角色都具有唯一地址。Cisco DNA Center 获知所有 PSN 地址，并且 Cisco DNA Center 用户将交换矩阵边缘节点交换机映射到支持每个边缘节点的 PSN。

有关 ISE 性能和规模的更多信息，请访问：https://cs.co/ise-scale。

Cisco DNA Center

SD-Access 解决方案的自动化以 Cisco DNA Center 为核心。SD-Access 通过作为 Cisco DNA Center 软件一部分运行的应用程序包启用，该软件用于设计、调配和应用策略，并通过网络状态感知使智能园区有线和无线网络的创建变得更加便捷。

Cisco DNA Center 对配置和运营工作流程的主要方面进行集中管理。

- **设计** - 配置设备全局设置、物理设备清单的网络站点配置文件、DNS、DHCP、IP 寻址、软件映像存储库和管理、设备模板以及用户访问。
- **策略** - 定义业务意图以便在网络中进行调配，包括创建虚拟网络，将终端分配到虚拟网络，为组定义策略合同以及配置应用策略。
- **调配** - 调配设备并将其添加到设备清单中以进行管理，支持思科即插即用服务，并创建交换矩阵域、控制平面节点、边界节点、边缘节点、交换矩阵无线网络、思科统一无线网络无线连接、传输网络连接和外部连接。
- **网络状态感知** - 使用网络、客户端和应用运行状况控制面板、问题管理和传感器驱动的测试，实现主动监控并获得洞察力，以确认用户体验符合配置意图。
- **平台** - 通过功能集捆绑包、配置、运行时控制面板和开发人员工具包，支持使用 API 以编程方式访问网络以及与第三方系统实现系统集成。

Cisco DNA Center 支持使用 API 实现集成。例如，可以通过 Cisco DNA Center 将 Infoblox 和 Bluecat IP 地址管理及策略实施与 ISE 集成。一系列全面的北向 REST API 可以实现自动化、集成和创新。

- 所有控制器功能都可以通过北向 REST API 获得。
- 组织和生态系统合作伙伴可以轻松开发新应用。
- 所有北向 REST API 请求均通过控制器 RBAC 机制进行管理。

要将设备自动部署到网络中，提供必要的速度和一致性来确保运营效率，Cisco DNA Center 是关键。使用 Cisco DNA Center 的组织在部署和维护网络时，可获得减少成本和降低风险的优势。

Cisco DNA Center 设备

Cisco DNA Center 软件（包括 SD-Access 应用程序包）设计为在 Cisco DNA Center 设备上运行。该设备提供多种外型规格，不仅可支持 SD-Access 应用程序，还可支持网络状态感知和可用的新功能。

如果您只部署了单一 Cisco DNA Center 设备，当该设备节点不可用时，该节点调配的 SD-Access 网络仍可正常工作，但在这个单一节点恢复正常前，将无法使用自动调配功能。若要实现高可用性，请配置具有同一设备类型的三个 Cisco DNA Center 设备，以形成一个三节点集群。Cisco DNA Center 集群可使用虚拟 IP 上托管的单个 GUI 接口进行访问，该接口由集群内可恢复的节点提供服务。配置单个节点时应考虑未来集群，以便在将来需要时能够轻松地支持多节点集群。

在三节点集群中，您可以启用服务分布，以自动提供分布式处理、数据库复制、安全复制和文件同步。软件升级也会在集群中的节点之间自动进行复制。集群在失去单个主机时仍可用，但需要两个主机才能保持正常运行。在三节点集群完全恢复正常前，某些维护操作（例如软件升级和从备份还原文件）会受到限制；在处于降级的双节点状态时，并非所有网络状态感知数据都会受到保护。

为了确保调配和网络状态感知通信效率，应在网络中靠近所管理设备数量最多的位置安装 Cisco DNA Center 集群，从而最大限度地减少设备的通信延迟。

有关 Cisco DNA Center 设备功能的其他信息，请参阅 Cisco.com 上的产品手册。

共享服务

端到端网络虚拟化的设计需要详细规划才能确保虚拟网络的完整性。在大多数情况下，需要使用某种形式的共享服务，而且该服务必须可以在多个虚拟网络间重复使用。必须正确部署这些共享服务才能使共享这些服务的不同虚拟网络之间保持相互隔离。使用直接连接到交换矩阵边界的融合路由器可以为跨多个网络的共享服务前缀路由泄漏提供一种机制，而防火墙的使用则可以提供额外一层安全防护和对虚拟网络间流量的监控。共享服务的示例包括:

- **无线基础设施** – 相较之前使用多个 SSID 隔离终端通信的低效策略而言，使用通用无线局域网（单个 SSID）可以提高射频性能和成本效益。在 WLC 上使用动态 VLAN 分配来分配专用 VLAN，使用 802.1X 身份验证将无线终端映射到相应的 VN 中，从而实现流量隔离。
- **DHCP、DNS 和 IP 地址管理** – 可以重复使用同一组基础设施服务，前提是它们支持虚拟网络。此支持包括高级 DHCP 作用域选择条件、完整的 DCHP 回应选项、多个域和重叠地址支持等特殊功能，以便将服务扩展到单个网络以外。
- **互联网接入** – 可将同一组互联网防火墙用于多个虚拟网络。如果需要防火墙策略对每个虚拟网络是唯一的，建议使用多情景防火墙。
- **IP 语音/视频协作服务** – 当多个虚拟网络中连接了 IP 电话和其他统一通信设备时，发往通信管理器的呼叫控制信号和这些设备之间的 IP 流量需要能够流经基础设施中的多个虚拟网络。

软件定义的接入架构

SD-Access 架构受面向园区实施的交换矩阵技术支持，因此客户可以使用在物理网络（底层网络）上运行的虚拟网络（重叠网络或交换矩阵重叠网络）来创建替代拓扑，从而进行设备连接。数据中心交换矩阵中的重叠网络通常用于通过虚拟机移动性提供第 2 层和第 3 层逻辑网络（示例：Cisco ACI™、VXLAN/EVPN 和 FabricPath）。此外，重叠网络也可用于在广域网络中从远程站点提供安全隧道（示例：MPLS、DMVPN 和 GRE）。此部分介绍有关 SD-Access 架构各元素的信息以及设计建议。

底层网络

底层网络由用于部署 SD-Access 网络的物理交换机和路由器定义。底层网络的所有网络元素都必须通过路由协议建立 IP 连接。SD-Access 的底层实施不是使用任意网络拓扑和协议，而是使用包含园区边缘交换机的精心设计的第 3 层基础（也称为路由接入层设计），以确保网络的性能、可扩展性和高可用性。

在 SD-Access 中，底层交换机支持面向用户的终端物理连接。但是，终端用户子网和终端不是底层网络的一部分，它们是可编程的第 2 层或第 3 层重叠网络的一部分。

经过验证的 SD-Access 解决方案支持 IPv4 底层网络，以及 IPv4 和 IPv6 重叠网络。

底层网络设计注意事项

精心设计底层网络有助于确保 SD-Access 网络的稳定性、性能和高效利用。可以使用 Cisco DNA Center 实现底层网络的自动化部署。

交换矩阵的底层网络具有以下设计要求:

- **第 3 层接入设计** – 将第 3 层路由网络用于交换矩阵可提供最高级别的可用性，而无需使用避免产生环回的协议或接口绑定技术。
- **增加默认 MTU** – VXLAN 报头添加 50 字节封装开销和可选的 54 字节封装开销。有些以太网交换机支持的最大传输单位 (MTU) 为 9216，而其他以太网交换机的 MTU 可能为 9196 或更小值。考虑到服务器 MTU 通常高于 9000 字节，启用 9100 的宽松网络 MTU 可确保以太网巨帧得以传输，而不会在交换矩阵内部和外部对其进行任何分段。
- **使用点对点链路** – 点对点链路可实现最快的收敛，因为其无需等待上层协议超时，而这种情况在更复杂的拓扑中却非常常见。点对点链路与推荐的物理拓扑设计相结合，可在链路出现故障后提供快速收敛。快速收敛是快速检测链路故障的一项优势，因为它可以触发立即使用预先存在于路由和转发表中的备用拓扑条目。请使用光纤技术实施点对点链路，不要使用铜缆，因为光纤接口可以提供最快的故障检测时间，从而缩短收敛时间。
- **ECMP** – 等价多路径路由是一种路由策略，它可以通过多个最佳路径来转发通往一个目的地的下一跳数据包。这些 ECMP 路径之间的负载均衡通过思科快速转发 (CEF) 自动执行。应通过 ECMP 感知 IGP 路由协议利用并行成本链路以及提供冗余转发路径以实现恢复能力。
- **BFD** – 应使用双向转发检测来增强 IGP 的故障检测和收敛特征。
- **NSF** – 不间断转发可与 SSO（状态切换）配合使用，在路由处理器 (RP) 切换的情况下提供数据包的连续转发。应使用 NSF 感知 IGP 路由协议，以最大限度地缩短切换后无法使用网络的时间。
- **交换矩阵专用的 IGP 流程** – 交换矩阵的底层网络只需要从交换矩阵边缘到边界节点的 IP 可访问性。在交换矩阵部署中，可以通过在 SD-Access 交换矩阵实施的专用 IGP 流程实施单区域 IGP 设计，通常使用 IS-IS 等链路状态协议，以获得性能优势。虽然 IS-IS 用于局域网自动化，但支持 OSPF 和 EIGRP 等其他路由协议，同时还支持 ECMP 感知和 NSF 感知。

- **环回传播** - 分配给底层设备的环回地址需要在交换矩阵外部传播，以便与交换矩阵控制平面节点、DNS、DHCP 和 AAA 等基础设施服务建立连接。实现 RLOC 可访问性需要使用 /32 主机掩码，且不可使用默认路由。在将主机路由引入网络时，向主机路由应用标记。引用标记，以便仅重新分发并传播已标记的环回路由。这样可以轻松地在交换矩阵外部选择性传播路由，并且无需维护前缀列表。
- **WLC 可访问性** - 应将与 WLC 的连接视为环回地址。AP 无法使用底层网络中的默认路由访问 WLC。在 AP 以物理方式连接的每台交换机的全局路由表中，必须存在通往 WLC IP 地址的特定路由。
- **局域网自动化部署** - 您可以通过在 Cisco DNA Center 中使用局域网自动化服务来自动配置底层网络。在非全新部署的情况下，您需要手动创建底层网络。手动创建的底层可与自动化底层部署有所不同（例如可以选择不同的 IGP），但前面列出的底层网络设计原则仍然适用。Cisco DNA Center 局域网自动化功能是适用于新网络的手动底层网络部署的替代方案，它采用 IS-IS 路由接入设计。虽然有许多备用路由协议，但选择 IS-IS 具备操作优势，例如在不存在 IP 协议依赖关系的情况下建立相邻关系，使用环回地址实现对等连接功能，以及对 IPv4、IPv6 和非 IP 流量执行不可知处理。
- 在最新版本的 Cisco DNA Center 中，局域网自动化利用思科网络即插即用功能在底层网络中部署单播和源特定组播路由配置，从而提高在此基础上构建的服务的流量传输效率。
- 使用局域网自动化功能自动部署底层网络，从而提供 MTU 协调、路由点对点链路、ECMP、NSF、BFD 和路由接入，并传播自动交换矩阵节点的环回地址。它还会调配 CLI 和 SNMP 凭证，同时使用 SWIM 将设备软件升级到所需的版本。
- 要自动部署底层网络，Cisco DNA Center 需要使用 IP 访问直接连接到新底层设备的思科网络即插即用种子设备。其余设备则使用逐跳 CDP 发现和调配进行访问。

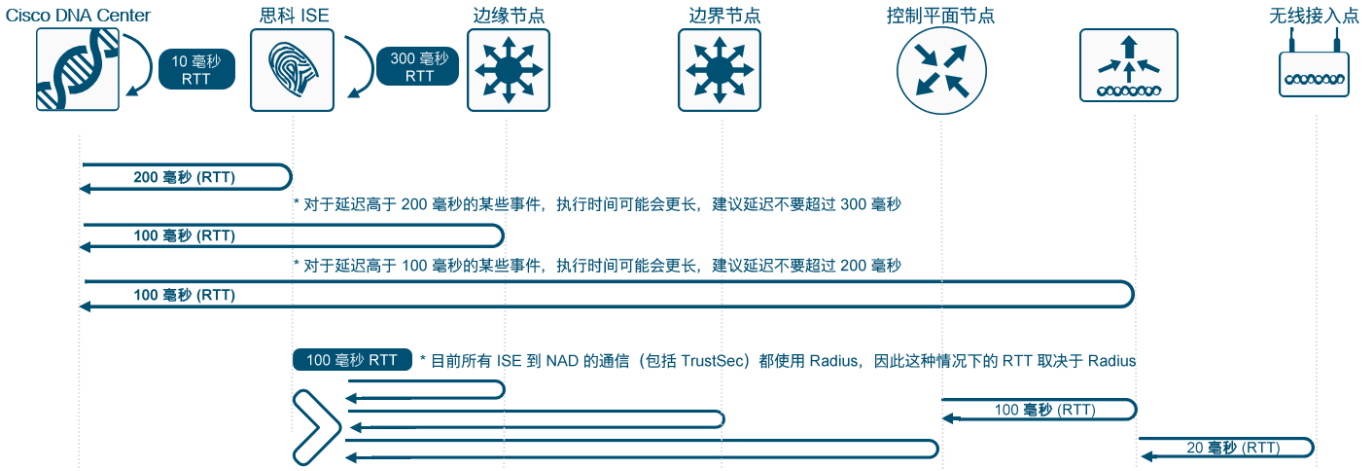
延迟注意事项

交换矩阵接入点在本地模式下运行。这要求 AP 和无线局域网控制器之间的 RTT（往返时间）不超过 20 ms。这通常意味着 WLC 部署在与无线接入点相同的物理站点中。如果物理站点和数据中心内的 WLC 之间存在专用的暗光纤，并规定了延迟要求，则 WLC 和 AP 可能位于不同的物理位置。这种情况通常出现在城域网以及用于分布式园区的 SD-Access 中。不应跨广域网通过 WLC 部署 AP。

Cisco DNA Center 3 节点集群的集群节点之间的 RTT 不得超过 10 毫秒。有关物理拓扑选项和故障转移场景，请参阅 Cisco DNA Center 3 节点集群高可用性场景和网络连接详细信息技术说明。

网络中的延迟对性能而言是一项重要的考虑因素，且必须将 Cisco DNA Center 及其管理的任何网络设备之间的 RTT 考虑在内。最佳 RTT 必须低于 100 毫秒，才能实现基础自动化、网络状态感知、软件定义接入以及 Cisco DNA Center 提供的所有其他解决方案的最佳性能。支持的最大延迟为 200 ms。支持 100 毫秒到 200 毫秒之间的延迟，但对于某些事件（包括资产收集、交换矩阵调配、SWIM 和其他进程），执行时间可能会更长。

图 2. Cisco DNA Center 和 SD-Access 网络要求

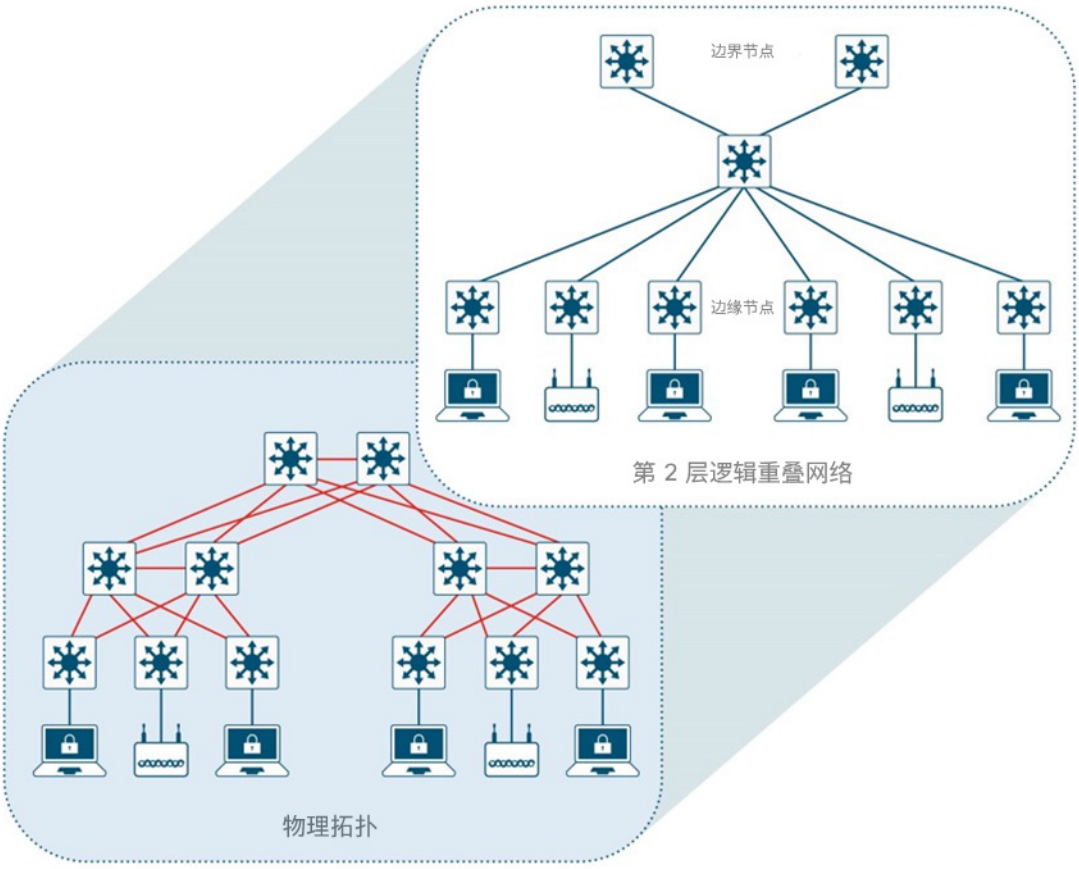


重叠网络

在底层网络的基础上创建重叠网络，以便创建虚拟网络。数据平面流量和控制平面信令都包含在每个虚拟网络内部，以保持网络之间的隔离，同时与底层网络保持独立。SD-Access 交换矩阵通过使用在交换矩阵边界起止的 IP 数据包将用户流量封装在重叠网络中，来实施虚拟化。交换矩阵边界包括交换矩阵的入口和出口边界、有线客户端的交换矩阵边缘交换机以及无线客户端的交换矩阵无线接入点。下文将详细介绍封装和交换矩阵设备角色。重叠网络可以跨所有底层网络设备运行，也可以跨其中一部分设备运行。多个重叠网络可以在同一个底层网络中运行，从而通过虚拟化提供多租户支持。每个重叠网络显示为一个用于连接到外部网络的虚拟路由和转发 (VRF) 实例。通过使用 VRF-Lite，您可在将网络扩展到交换矩阵外部时保留重叠网络隔离，从而在连接到交换矩阵的设备内以及支持 VRF 的设备之间的链路上维持网络隔离。

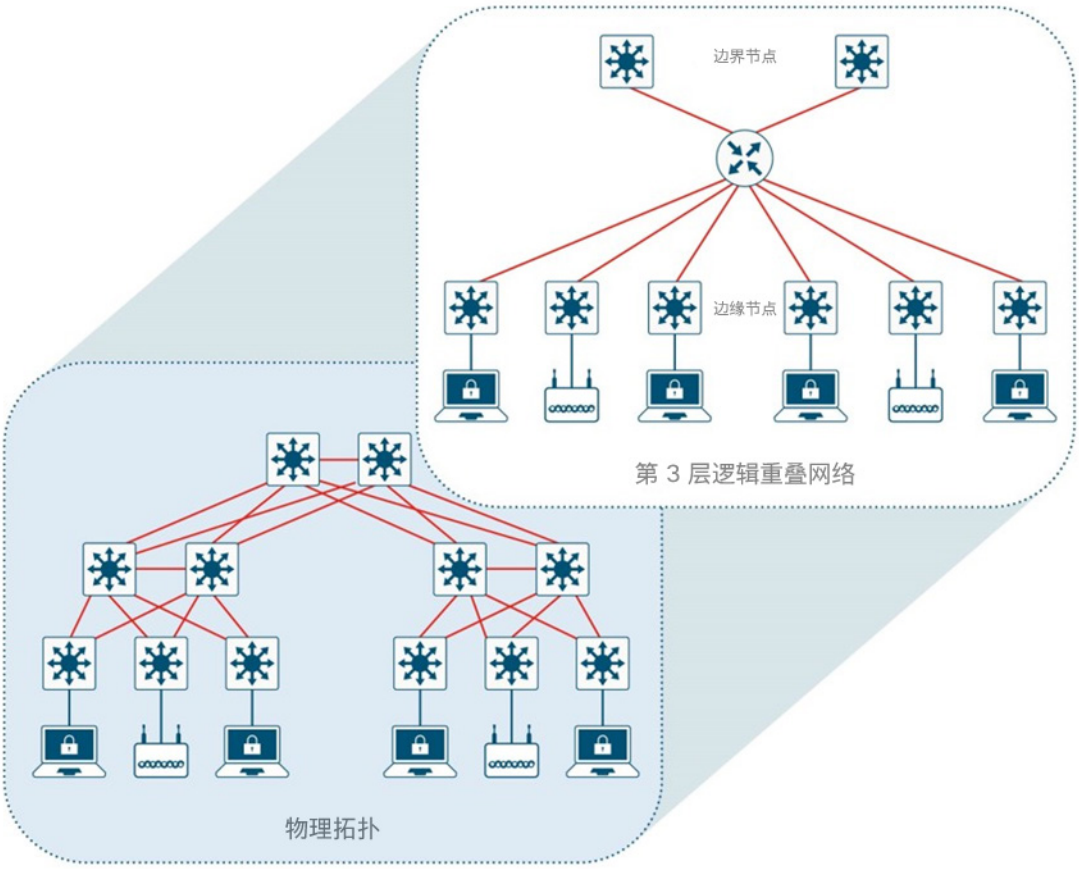
第 2 层重叠网络模拟局域网分段以传输第 2 层帧，从而在第 3 层底层网络上负载单个子网。第 2 层重叠网络在模拟物理拓扑时非常有用，但可能会受到第 2 层泛洪的影响，具体取决于设计。默认情况下，SD-Access 支持在没有第 2 层广播泛洪和未知组播流量的情况下传输 IP 帧，从而改变行为并减少传统局域网的限制，以便能够创建更大的子网。“SD-Access 解决方案组件” 部分介绍在不从交换矩阵边缘广播的情况下让 ARP 正常工作所需的交换矩阵组件，这是通过使用交换矩阵控制平面进行 MAC 到 IP 地址表查找实现的。

图 3. 第 2 层重叠网络 - 逻辑交换连接



第 3 层重叠网络从物理连接中抽象出基于 IP 的连接，使多个 IP 网络能够成为每个虚拟网络的一部分。

图 4. 第 3 层重叠网络 - 逻辑路由连接



交换矩阵中的组播转发

在早期版本的 SD-Access 中，对于有线和无线终端，重叠网络范围内的 IPv4 组播转发通过将组播数据包*前端复制*到交换矩阵中实现；这意味着边界（前端）必须获取每个组播数据包，并且对于每个边缘接收方交换机，必须复制数据包并进行转发。最新版本的 SD-Access 可以选择将底层组播功能与许多平台配合使用（无论是手动配置还是通过使用局域网自动化实现），从而使用内置于交换矩阵设备中的组播复制功能更高效地将流量传送到相关边缘交换机，而不会因对前端复制进行额外处理而增加边界的负担。组播会封装到相关交换矩阵边缘交换机，这些交换机将解封组播并将其复制到交换机上的所有相关接收方。如果接收方是无线终端，交换矩阵边缘会向与组播接收方关联的 AP 封装组播（就像单播一样）。

组播源可以位于重叠网络中，也可以位于交换矩阵外部。对于 PIM 部署，重叠网络中的组播客户端在属于重叠网络终端地址空间的交换矩阵边界使用交汇点 (RP)。Cisco DNA Center 配置所需的组播协议支持。

技术提示
SD-Access 解决方案支持 PIM 源特定组播和 PIM 稀疏模式（任意源组播）。重叠 IP 组播通常需要借助边界在交换矩阵重叠网络中调配 RP。通过在 RP 之间实施 MSDP，可以实现 RP 冗余。有关组播优化（例如底层组播复制），请参阅版本说明了解特定平台的可用性。

除通信效率外，在底层网络中配置组播还可实现具有第 2 层泛洪选项的重叠网络。SD-Access 第 2 层泛洪选项使用底层网络中的源特定组播，将 ARP 帧、广播帧和链路本地组播帧复制到重叠网络中的所有终端。启用后，第 2 层泛洪可支持 mDNS 和类似服务，并满足某些静默主机终端在激活通信之前要求接收特定非单播流量的连接需求。

重叠交换矩阵设计注意事项

在 SD-Access 交换矩阵中，重叠网络用于传输交换矩阵内的用户流量。交换矩阵封装还携带用于重叠网络内流量分段的可扩展组信息。部署虚拟网络时，请在您的设计中考虑以下因素:

- **根据网络要求按需进行虚拟化** – 使用 SGT 进行分段可以简化基于组的策略的管理，并能在虚拟网络内部的终端组之间实现精细的数据平面隔离，从而满足诸多网络策略要求。使用 SGT 还可实现策略的可扩展部署，而无需根据 IP 地址对策略进行繁琐更新，此类更新可能容易遭到破坏。虚拟网络支持传输 SGT 用于组分段。当网络要求指定在数据平面和控制平面都进行隔离时，应使用虚拟网络。对于此类情况，如果不同虚拟网络间需要进行通信，则使用外部防火墙或其他设备来实现虚拟网络间通信。您可以选择其中一个选项或同时选择两个选项来满足您的要求。
- **减少子网并简化 DHCP 管理** – 在重叠网络中，可以跨交换矩阵扩展 IP 子网，而不会出现大型第 2 层网络上可能发生的泛洪问题。请使用较少的子网和 DHCP 作用域来简化 IP 寻址和 DHCP 作用域管理。子网的大小取决于它们支持的服务，而不受网关位置的限制。启用可选的广播泛洪功能时，可以根据特定部署中流量组合的其他带宽和终端处理要求来限制子网大小。
- **避免重叠的 IP 子网** – 不同的重叠网络可以支持重叠的地址空间，不过请注意，大多数部署都需要跨所有虚拟网络的共享服务和其他虚拟网络间通信。请避免地址空间重叠，这样就不需要为共享服务和 VN 间通信添加网络地址转换设备，也就不会增加运营复杂性。

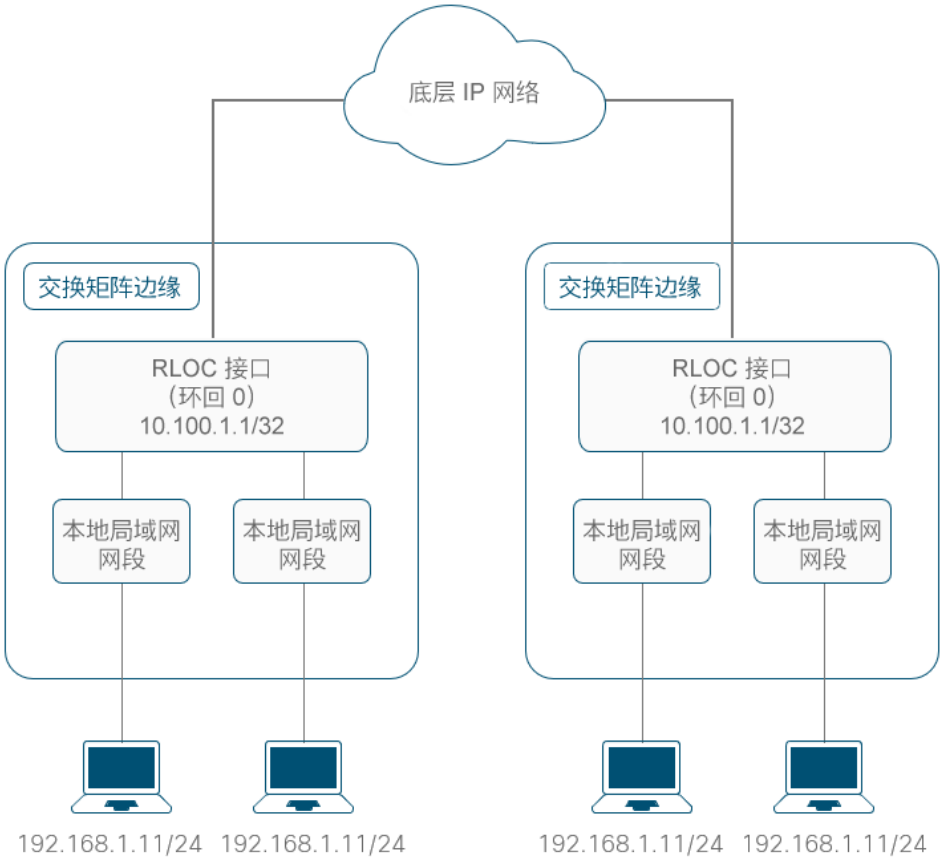
交换矩阵数据平面和控制平面

SD-Access 使用虚拟可扩展局域网 (VXLAN) 技术框架为交换矩阵数据平面封装配置重叠网络。VXLAN 封装整个底层网络中的第 2 层帧以跨底层网络进行传输，并使用 VXLAN 网络标识符 (VNI) 标识各重叠网络。VXLAN 报头还携带微分段所需的 SGT。

映射和解析终端地址功能需要控制平面协议，而 SD-Access 使用定位/ID 分离协议 (LISP) 执行此任务。LISP 不仅基于作为设备终端标识符 (EID) 的 IP 地址或 MAC 地址进行路由，还可基于由 LISP 提供作为用于表示该设备网络位置的路由定位符 (RLOC) 的其他 IP 地址进行路由，从而实现了路由优势。EID 和 RLOC 组合提供所有必要的流量转发信息，即使终端在不同的网络位置出现时使用不变的 IP 地址也是如此。同时，终端身份与其位置的分离也实现了在多个第 3 层网关的后面使用同一 IP 子网中的地址，而不是使用传统网络中 IP 子网与网关的一对一耦合。

下图显示属于重叠网络的两个子网的示例。子网在物理分离的第 3 层设备之间延伸。RLOC 接口是属于同一子网或不同子网的终端之间建立连接所需的唯一可路由地址。

图 5. 示例拓扑 - 子网延伸



有关交换矩阵控制平面和数据平面结构的详细信息以及术语表，请参阅附录。

交换矩阵数据和控制平面设计注意事项

设计交换矩阵数据平面和控制平面时，需要考虑以下关键要求：交换矩阵控制平面设计、交换矩阵边界设计和基础设施服务。

交换矩阵控制平面节点设计注意事项

交换矩阵控制平面包含用于为交换矩阵元素标识终端位置的数据库。要让交换矩阵正常工作，这是一项主要的关键功能。控制平面过载并响应缓慢会导致初始数据包发生应用流量丢失。如果交换矩阵控制平面出现故障，交换矩阵内的终端就无法与在本地数据库中尚不存在的远程终端建立通信。

Cisco DNA Center 将自动配置控制平面的功能。若要实现冗余，您应部署两个控制平面节点，由于每个节点都包含一个重复的控制平面信息副本，这样可以确保交换矩阵的高可用性。应该选择支持控制平面的设备，以根据交换矩阵终端支持组织的 HTDB、CPU 和内存需求。

如果所选边界节点支持交换矩阵的预期终端扩展要求，合理的做法是并置使用交换矩阵控制平面功能和边界节点。但是，如果无法实现并置选项（例如：Nexus 7700 边界缺少控制平面节点功能或终端扩展要求超出平台能力），则可以添加专用于此功能的设备，例如在交换矩阵站点添加物理路由器或虚拟路由器。要将控制平面功能分离到专用设备，支持在交换矩阵边缘节点之间频繁漫游终端是另一个需要考虑的因素。在交换矩阵边缘节点之间漫游会导致一些控制平面事件，牵涉到 WLC 会根据这些漫游终端的移动情况更新控制平面节点。通常情况下，网络中的核心交换机形成 SD-Access 交换矩阵的边界；建议不要在高频漫游环境下将控制平面功能添加到这些边界节点中，因为它会影响交换矩阵网络的核心层和边界功能。

在纯有线部署中，SD-Access 交换矩阵站点最多可支持六个控制平面节点。思科 AireOS 和 Catalyst WLC 可以与站点中的四个控制平面节点通信。要在具有 SD-Access 无线部署的站点中使用四个控制平面节点，需要将两个控制平面节点专用于访客（稍后讨论），并将另外两个节点专用于本地站点流量。如果未使用专用访客边界/控制平面节点功能，则在每个交换矩阵站点中，WLC 只能与两个控制平面节点通信。

交换矩阵边界节点设计注意事项

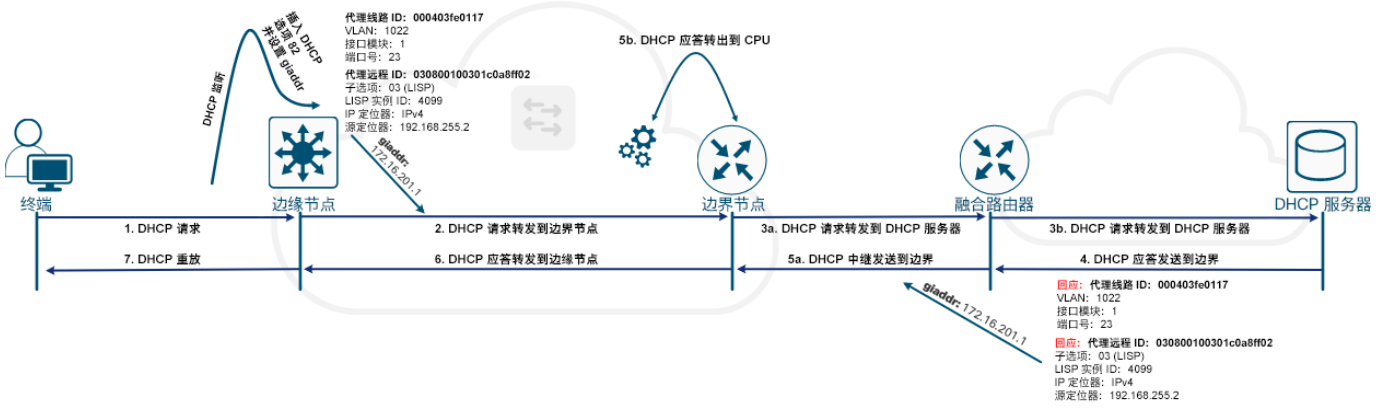
交换矩阵边界的设计取决于交换矩阵与外部网络的连接方式。交换矩阵内的 VN 应该映射到交换矩阵外的 VRF-Lite 实例。根据共享服务在网络中的位置，可能需要调整边界设计。

与传输控制平面互联时，可以使用本地站点服务进行大型分布式园区部署。在这些新角色成为一项通用特性后，您可以搜索本主题获取指导。

基础设施服务设计注意事项

SD-Access 不需要对现有基础设施服务进行任何更改，但交换矩阵边界设备应该已经实施了用于处理 DHCP 中继功能差异的功能以辅助交换矩阵部署。在典型的 DHCP 中继设计中，除了 DHCP 服务器应该将提议的地址定向到的位置以外，唯一网关 IP 地址还决定了为终端分配的子网地址。在交换矩阵重叠网络中，该网关并非唯一，重叠网络内的所有交换矩阵边缘设备上都存在相同的任播 IP 地址。未在边界节点上进行特殊处理或未由 DHCP 服务器本身进行特殊处理，通过边界从 DHCP 服务器返回的 DHCP 提议可能无法正确中继到发出 DHCP 请求的交换矩阵边缘交换机。

图 6. 交换矩阵 DHCP 数据包流



为了标识特定的 DHCP 中继源，Cisco DNA Center 在交换矩阵边缘使用 DHCP 选项 82（包括线路 ID 插入信息选项）自动配置中继代理。添加信息可提供额外的子选项，用于标识特定的源中继代理。线路 ID 中嵌入的 DHCP 中继信息由具有高级 DHCP 边界中继功能的交换矩阵边界或 DHCP 服务器本身用作应答请求方的 DHCP 提议的目的。

如果使用具有高级 DHCP 边界中继功能的边界，DHCP 服务器作用域配置相对于包含交换矩阵终端的作用域可保持不变，而不是创建标准的非交换矩阵作用域。当您使用具有此附加 DHCP 功能的边界节点时，边界节点将检查从 DHCP 服务器（不得使用未回应此选项的 DHCP 服务器）返回的 DHCP 提议。这些提议包括原始 DHCP 请求的交换矩阵边缘

交换机源的 RLOC（在提议中保留并返回）。收到 DHCP 提议的边界节点引用包含 RLOC 信息的嵌入线路 ID 并将 DHCP 提议定向回正确的中继目的。

无线功能

SD-Access 支持用于将无线接入集成到网络的两个选项。其中一个选项是使用传统思科统一无线网络本地模式配置“机顶盒设备”作为非本地服务。在此模式下，SD-Access 交换矩阵只是用于无线流量的传输网络，这在迁移过程中可能十分有用，可从 AP 将 CAPWAP 隧道终端流量传输到 WLC。另一个选项是完全集成的 SD-Access 无线，可扩展 SD-Access 优势以包括无线用户；使用此选项时，终端流量在交换矩阵边缘交换机直接加入交换矩阵。

您可以使用两个附加组件（交换矩阵无线控制器和交换矩阵模式 AP）在本地将无线功能集成到 SD-Access 中，从而获得无线传输的优势。受支持的思科无线局域网控制器 (WLC) 配置为交换矩阵无线控制器，以便与交换矩阵控制平面通信，从而注册第 2 层客户端 MAC 地址、SGT 和第 2 层 VNI 信息。交换矩阵模式 AP 是与交换矩阵无线控制器关联的采用思科 WiFi6 以及第二代和第一代 802.11ac 技术的 AP，它配置有支持交换矩阵的 SSID。这些 AP 负责与无线终端通信，在有线域中，这些 AP 还协助 VXLAN 数据平面封装和解封相连接的边缘节点上的流量。

交换矩阵无线控制器使用与传统集中式模型（即本地模式控制器）相同的模型来管理和控制交换矩阵模式 AP，提供移动性控制和射频资源管理等同样的运营优势。其显著区别是从交换矩阵 SSID 中的无线终端传输的客户端流量无需进行无线接入点控制和调配 (CAPWAP) 封装并从 AP 转发到中央控制器。相反，来自无线客户端的通信由交换矩阵连接的 AP 进行 VXLAN 封装。正是因为这种区别，具有集成 SGT 功能的分布式数据平面才得以实现。流量通过 SD-Access 交换矩阵采取最佳路径传输到目的，并且无论是有线还是无线终端连接都使用一致的策略。

AP 的控制平面通信使用通往 WLC 的 CAPWAP 隧道，类似于传统的思科统一无线网络控制平面。不过，WLC 与 SD-Access 控制平面的集成支持无线客户端在整个交换矩阵中的不同 AP 之间漫游。如果与新 RLOC 关联的无线客户端 EID 发生任何更改，SD-Access 交换矩阵控制平面都会相应更新其主机跟踪数据库，因此本身就支持漫游功能。

虽然当无线流量在交换矩阵的无线和有线部分之间移动时，会使用交换矩阵模式 AP 对该流量进行 VXLAN 流量封装，但这些 AP 并非边缘节点。相反，这些 AP 使用 VXLAN 封装直接连接到边缘节点交换机，并依靠这些交换机提供第 3 层任播网关等交换矩阵服务。AP 可以直接连接到边缘节点交换机，也可以连接到扩展节点交换机。AP 使用 VXLAN 封装通过隧道传输无线数据流量，并依靠交换矩阵边缘节点交换机提供第 3 层任播网关等交换矩阵服务。

将无线局域网集成到交换矩阵中可以让无线客户端享受到交换矩阵的优势，包括寻址简化、通过扩展子网实现移动，以及跨有线和无线域的基于策略一致性的端到端分段。此外，无线集成使 WLC 无需再执行数据平面转发，而继续充当无线域的集中式服务和控制平面。

访客无线服务

如果您没有部署思科统一无线网络无线机顶盒设备，并需要交换矩阵无线访客接入服务连接到互联网，请通过创建支持访客 SSID 的专用虚拟网络，将无线访客服务与其他网络服务隔离。使用 VRF Lite 或类似技术，扩展交换矩阵边界和 DMZ 之间的访客流量隔离。

访客流量可以在其自己的虚拟网络中终止，并且该虚拟网络可以通过传统方法从边界扩展到 DMZ。此类部署不需要在数据中心部署任何访客锚点。

在 SD-Access 交换矩阵网络中部署访客接入的另一种方式是使用访客边界/控制平面。访客流量从交换矩阵边缘节点直接封装到 DMZ 中的访客边界/控制平面节点，从而实现与其他企业数据流量的完全隔离。

Cisco DNA Center 自动执行并管理仅用于为交换矩阵设备实施无线访客解决方案的工作流程，但有线访客服务不包括在该解决方案中。

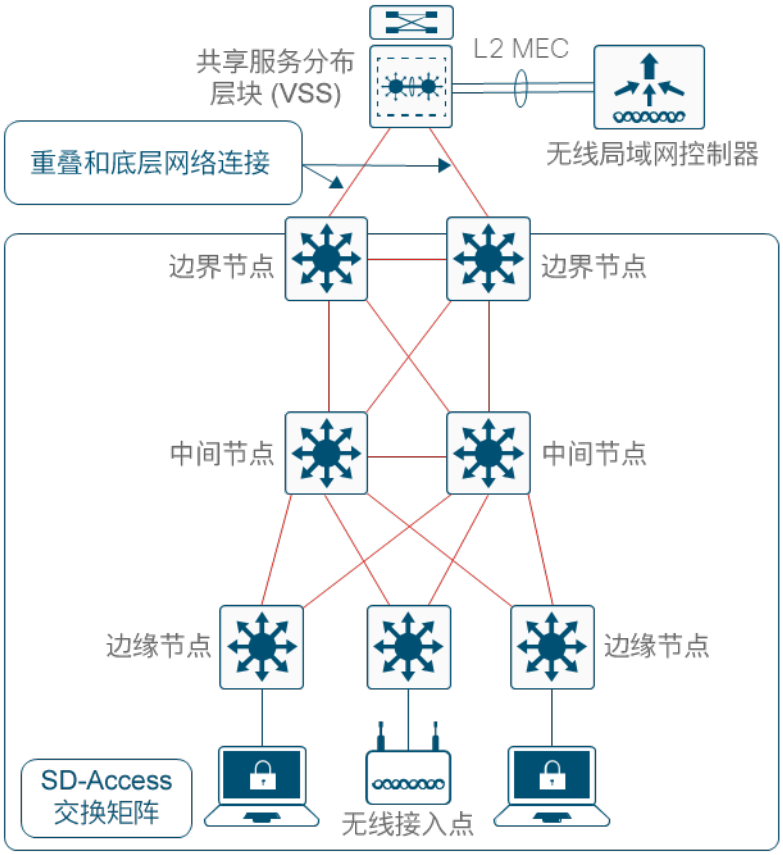
交换矩阵无线集成设计注意事项

将交换矩阵 WLC 和交换矩阵模式 AP 集成到 SD-Access 架构中时，交换矩阵 WLC 并非主动参与数据平面流量转发，而是由交换矩阵模式 AP 负责将无线客户端流量传入和传出有线交换矩阵。WLC 控制平面保留了很多本地模式控制器的特征，包括需要在 WLC 与 AP 之间建立低延迟连接的要求。托管要求使得交换矩阵 WLC 不可能跨典型广域网成为远程站点上的交换矩阵模式 AP 的控制器。因此，远程站点如果要与具有集成无线功能的 SD-Access 通信，需要在该站点有一个本地控制器。

将无线功能集成到 SD-Access 中时，另一个注意事项是交换矩阵 WLC 的位置和连接。在规模较大的部署中，WLC 通常连接到属于底层网络一部分的共享服务分布层块。首选的分布层块应该有机箱冗余能力，并能支持与 WLC 的第 2 层多机箱 EtherChannel 连接，确保实现链路和平台冗余。通常，我们使用虚拟交换系统或交换机堆叠来实现这些目标。

AP 连接到名为 INFRA_VRF 的预定义 VRF，这就是扩展节点基础设施设备用于连接的 VRF。VRF 已连接到全局路由表，从连接设备到边界的通信通过底层网络进行，且这些设备的可连通性必须在外部通告。这种设计允许 WLC 的网络连接保持不变，同时仍然能够在交换矩阵域边缘管理 AP。

图 7. 将无线组件集成到 SD-Access 中



无线机顶盒设备集中式无线选项设计注意事项

在无法将无缝漫游区域中的 WLC 和无线接入点专门用于加入交换矩阵的情况下，可以选择传统的思科统一无线网络设计模型，它也称为本地模式模型。SD-Access 与思科统一无线网络 “机顶盒设备” 兼容，后者作为非本地服务选项，不具备交换矩阵集成的优势。

机顶盒设备集中式设计仍可提供 IP 地址管理、简化的配置和故障排除，以及大规模漫游等优势。在集中式模型中，WLAN 控制器和无线接入点均位于同一个站点内。您可以将 WLAN 控制器连接到数据中心服务块或邻近园区核心的专用块。无线局域网客户端和局域网之间的无线流量将使用控制器与 AP 之间的无线接入点控制和调配 (CAPWAP) 协议进行隧道传输。AP 可以驻留在交换矩阵内部或外部，无需对推荐的集中式 WLAN 设计进行任何更改。务必谨记，在交换矩阵仅用作机顶盒传输设备时，交换矩阵和 SD-Access 的优势不会扩展到无线网络，同时二者也不会与无线网络集成。

有关园区无线设计的其他信息，请参阅园区局域网和无线局域网设计指南。

混合 SD-Access 无线和集中式无线选项设计注意事项

在将 SD-Access 无线集成到交换矩阵之前，许多组织可能会将部署具有集中式无线机顶盒设备的 SD-Access 作为过渡的第一步。在这种情况下，组织应将一个 WLC 专用于支持 SD-Access 无线。借助专用于 SD-Access 的 WLC，可在交换矩阵域和非交换矩阵域中使用相同的 SSID，而无需通过做出改变（例如新的软件版本和 AP 组配置）来修改现有的集中部署。

组织可以在迁移阶段部署集中式和 SD-Access 无线服务。如果不要求当前部署的集中式无线软件和配置保持不变，则 Cisco DNA Center 可以自动执行新的安装，在同一 WLC 上同时支持两项服务。在这种情况下，从 Cisco DNA Center 进行的新安装不会考虑现有的运行配置，相反，Cisco DNA Center 会自动创建新的替换服务。

安全策略设计注意事项

每个组织的安全策略各不相同，想要定义一种放之四海而皆准的安全设计根本不可能。安全设计必须以信息安全策略和法律合规性为导向。安全设计的规划阶段对于确保在安全和用户体验之间达到恰到好处的平衡具有重要作用。为 SD-Access 网络设计安全策略时，应该考虑以下几个方面：

- 网络的开放性：有些组织只允许网络中存在组织发放的设备，而另一些组织则支持“自带设备”方案。或者，您也可以部署“自选设备”模型，即向用户提供列入列表的 IT 核准终端供业务使用，以此平衡用户选择并实现更易于管理的终端安全防护。此外，还可以采用基于身份的方案，根据设备的所有权部署网络安全策略。例如，组织发放的设备可以获得基于组的访问权限，而个人设备只能接入互联网。
- 身份管理：最简单的身份管理是使用用户名和密码对用户进行身份验证。添加嵌入式安全功能和对网络设备的应用可视性后，可以为高级策略定义提供遥感勘测数据。高级策略定义包括一些其他情景信息，例如物理位置、使用的设备、接入网络的类型、使用的应用，以及一天的时间。
- 身份验证、授权和记账策略：身份验证是建立并确认请求接入网络的客户端身份的过程。授权是授权终端访问某组网络资源的过程。分段策略不一定必须在接入层实施，而是可以部署在多个位置。在交换矩阵边缘节点实施策略，将 SGACL 用于 VN 内的分段，并通过动态 VLAN 分配将终端映射到 VN 中。可使用事件日志、ACL 命中计数器和类似的标准记帐工具增强可视性。
- 终端安全：终端可能会感染恶意软件，危害数据并造成网络中断。通过恶意软件检测、终端管理和从网络设备导出数据，可以帮助用户洞察终端的行为。网络与安全设备和分析平台紧密集成，可为网络提供隔离并帮助修复受感染设备所需的必要情报。
- 数据完整性和机密性：使用虚拟网络的网络分段可控制对应用的访问，例如将员工事务与物联网流量隔离；在交换环境中使用 IEEE 802.1AE MACsec 对数据路径进行加密，则可在第 2 层提供加密功能，用于防止窃听并确保数据无法被修改。
- 网络设备安全：增强网络设备的安全性至关重要，因为它们通常是安全攻击的目标。使用最安全的设备管理选项（例如启用使用 TACACS+ 的设备身份验证和禁用不必要的服务）是确保网络设备得到保护的最佳实践。

在每个虚拟网络内启用基于组的分段可以简化分层网络策略。使用虚拟网络可以实现相互隔离的控制和数据平面的网络级策略范围，在虚拟网络内使用 SGT 可以实现组级别的策略范围，从而跨有线和无线交换矩阵应用通用的策略。

SGT 能够根据角色或功能在网络内标记终端流量，并遵守基于角色的策略或在 ISE 上集中定义的 SGACL。在许多部署中，Active Directory 用作存储用户帐户、凭证和组成员身份信息的身份库。成功获得授权后，可以根据该信息对终端分类，并将终端分配到相应的可扩展组。然后，可以使用这些可扩展组创建分段策略和虚拟网络分配规则。

SGT 信息通过几种形式在网络中传输:

- 在 SD-Access 网络内部 - SD-Access 交换矩阵报头传输 SGT 信息。交换矩阵边缘节点和边界节点可以强制 SGACL 实施安全策略。
- 在交换矩阵外部具有思科 TrustSec 功能的设备上 - 具有思科 TrustSec 功能的内联设备在第 2 层帧的 CMD 报头中传输 SGT 信息。这是推荐的 SD-Access 网络外部传输模式。
- 在交换矩阵外部不具有思科 TrustSec 功能的设备上 - 可以借助 SXP 通过 TCP 连接传输 SGT。使用此方法可以绕过不支持 SGT 内联的网络设备。

有关思科 TrustSec 的其他信息，请参阅 https://cisco.com/go/trustsec。

解决方案管理

在 SD-Access 中部署交换矩阵并不需要全面了解 LISP 和 VXLAN，也不需要详细了解如何配置每一个网络组件和功能以便让 SD-Access 提供一致的端到端行为，而是使用 Cisco DNA Center（一种直观的集中管理系统）跨有线和无线 SD-Access 网络设计、调配和应用策略。

除了用于 SD-Access 的自动化功能外，Cisco DNA Center 还如 “解决方案组件” 部分所列，提供可提高组织效率的传统应用（例如软件映像管理）和一些新功能（例如设备运行状况控制面板和 360° 视图）。

Cisco DNA Center 是 SD-Access 的必备基础组件，支持将设备自动部署到网络中，从而提供确保运营效率所需的速度和一致性。组织在部署和维护网络时，可获益于减少的成本和降低的风险。

基于身份服务的策略管理使用由思科身份服务引擎 (ISE) 托管的外部存储库集成到 SD-Access 网络中。ISE 与 Cisco DNA Center 相结合，可以将用户和设备动态映射到可扩展的组并简化端到端安全策略管理和实施，而且实施规模比依靠 IP 访问列表的传统网络策略实施更大。

思科 SD-Access 站点参考模型

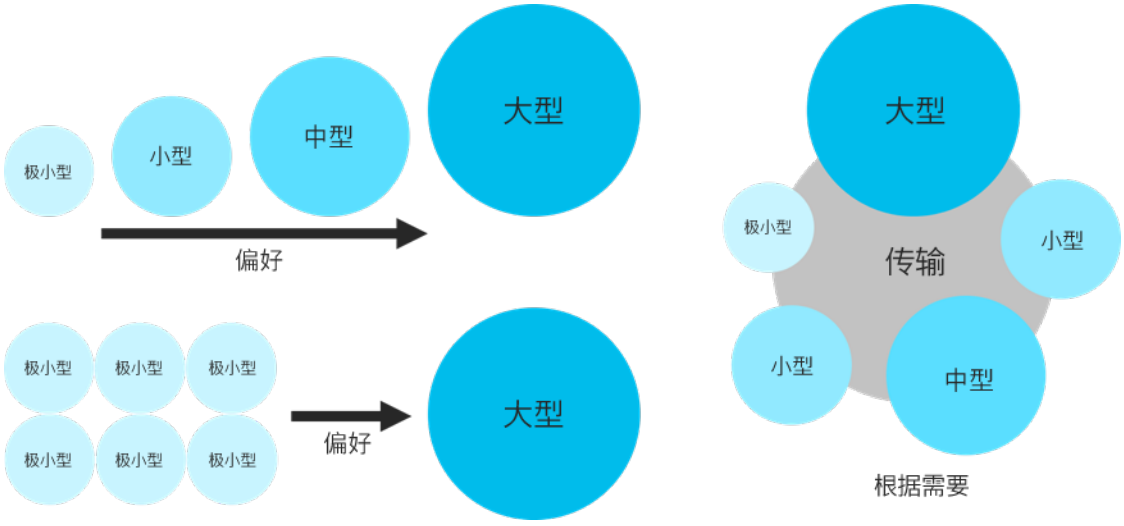
思科 SD-Access 交换矩阵的设计非常灵活，可以适应许多环境，这意味着它不是一种放之四海皆准的设计主张。交换矩阵的规模可以小到单个交换机或交换机堆叠，也可以大到一个或多个三层园区部署。SD-Access 拓扑应该将网络划分为模块化的组，并遵守与分层设计相关的相同设计原则和最佳实践，如园区局域网和无线局域网设计指南所述。

您要采用模块化设计创建可在整个网络中复制的设计元素。一般而言，SD-Access 拓扑应部署为分支网络，让交换矩阵边界节点位于分支的出口点中心。随着网络规模越变越大，会使用更加多样化的物理拓扑来满足专用网络服务部署的要求。

站点大小设计策略

SD-Access 设计的一个实际目标是在 Cisco DNA Center 的极限内以及在实现站点高可用性所需参数的范围内最大限度地增加交换矩阵站点的大小，同时最大限度地减少站点总数。使用之前 “SD-Access 解决方案组件” 部分中的元素创建站点。

图 8. 站点大小设计策略



SD-Access 设计注意事项

在设计用于 SD-Access 的网络时，除业务需求和驱动因素之外，还必须考虑多个技术因素，考虑这些因素后所得出的结果可用于制定网络中所用拓扑和设备的框架。这些因素并不是孤立的，而是必须从多个方面整体考量的项目，且不能严格隔离开来。

- 全新环境部署或现有环境部署
- 用户数量
- 地理位置
- 服务位置
- 传输类型
- 融合路由器
- 统一策略
- 站点生存能力
- 高可用性

全新环境部署和现有环境部署

必须考虑是全新环境部署还是现有环境部署，因为现有环境部署的目标是将其用于 SD-Access 网络。尽管迁移通过以下方法之一实现，但它不在本文档讨论范围内：

- **边界自动化 - 第 2 层切换** - SD-Access 的这一功能将传统网络与 SD-Access 网络连接，从而有效地将传统网络后面的主机添加到 SD-Access 交换矩阵。此设计在采用第二种方法时为临时使用案例。
- **按楼宇或按楼层** - 现有网络区域转换为 SD-Access。这通常按配线柜、楼层或楼宇来完成。一次至少迁移一个交换机。不支持一次迁移一个 VLAN，因为 VLAN 可能跨越多个传统交换机。

用户数量

除现有布线之外，设备和拓扑的最大驱动因素是整个位置的有线和无线客户端总数。这将确定所需的物理交换机端口数和无线接入点数，而这可能最终会产生对三层或两层网络设计的需求。客户端数量足够小时，网络可能由一个交换机堆叠组成。

地理位置

物理地理位置会影响网络设计。它不会对站点本身的拓扑产生直接影响，但必须将地理位置考虑在内，因为其与传输类型、服务位置、生存能力和高可用性相关。

位于同一城域网 (MAN) 内的位置或具有物理位置邻近的多个楼宇和直接互联光纤的园区，均可受益于用于分布式园区的 SD-Access 网络设计。延伸开来，即可以在各个位置之间实现本地统一策略，并有可能提供单一服务块位置。

跨 WAN 或互联网连接的位置还必须考虑服务和策略，以及交换矩阵重叠网络外部用于连接它们的路由基础设施。

共享服务

DHCP、DNS、ISE 和 WLC 等服务是 SD-Access 网络中的客户端所必需的元素。服务通常以三种方式中的一种方式进行部署。

在用于分布式园区的 SD-Access 中以及跨 WAN 分布的位置中，服务通常在本地数据中心部署。这些数据中心通常连接到中心位置（在本文档中称为总部 - HQ）的核心层或分布层。流量从远程站点和分支站点发送回总部，然后定向至必要的服务。

服务可能会位于该位置本地。出于生存能力目的，可以在每个交换矩阵站点位置建立服务块。本地服务可确保这些关键服务不会通过 WAN/MAN 发送，并确保终端能够访问它们，即使在 WAN 中出现拥塞或链路断开时也是如此。但是，这也需要在每个位置配备一个融合路由器来提供对共享服务的访问。

传输类型

传输只是交换矩阵站点之间的物理连接。这种连接可以是 MAN、WAN 或互联网。WAN 可以是 MPLS、IWAN 或其他 WAN 变体形式。在 Cisco DNA Center 内，传输称为 SD-Access 传输、基于 IP 的传输或 SD-WAN 传输。

SD-Access 传输用于适用于分布式园区的 SD-Access。使用 SD-Access 传输时，使用交换矩阵 VXLAN 封装（传输宏策略结构和微策略结构）在站点之间封装数据包。

在基于 IP 的传输中，数据包从交换矩阵 VXLAN 解封到本地 IP 中。解封到本地 IP 中后，使用传统的路由和交换模式转发这些数据包。在 Cisco DNA Center 中，基于 IP 的传输调配有 VRF Lite，可用于连接到上游设备。基于 IP 的传输通过两种方式实现：通过融合路由器连接到共享服务，以及通过连接到上游路由基础设施实现与 WAN 和互联网的连接。

虽然 VRF Lite 的配置在这些使用案例中具有相同的格式，但上游设备有所不同，因此引用时所用的名称也不同。当设备将交换矩阵边界节点连接到共享服务时，它称为融合路由器。当上游设备提供与 WAN 或互联网的连接时，它仅称为路由器或称为路由基础设施。

SD-WAN 传输通过支持 SD-WAN 的路由器连接交换矩阵站点。SD-WAN 传输的设计不在本文档讨论范围内。

融合路由器

融合路由器这一通用术语来自 MPLS 第 3 层 VPN。基本概念是，由于静态路由配置或通过路由对等，融合路由器知道每个 VPN (VRF) 中可用的前缀，因此可以将这些路由融合在一起。通用融合路由器的职责是在单独的 VRF 之间路由流量（VRF 泄漏），或将往返 VRF 的流量路由到全局路由表中的 DHCP 和 DNS 服务器等共享资源池中（路由泄漏）。这两项职责都涉及将路由从一个路由表移到一个单独的 VRF 路由表中。

在 SD-Access 部署中，融合路由器具有单一责任：为交换矩阵中的终端提供对共享服务的访问。根据共享服务的部署方式，有两种主要的方法来完成此任务。当共享服务路由在 GRT 中时，使用第一个选项。在融合路由器上，使用 IP 前缀列表匹配共享服务路由，路由映射引用 IP 前缀列表，VRF 配置引用路由映射，以确保仅泄漏特定匹配路由。第二个选项是将共享服务放在融合路由器上的专用 VRF 中。将共享服务放在一个 VRF 中，而将交换矩阵终端放在其他 VRF 中时，路由目标会在它们之间泄漏。

融合路由器可以是真正的路由平台、第 3 层交换平台或必须满足多个技术要求的防火墙。它必须支持：

- 多个 VRF
- 802.1q 标记（VLAN 标记）
- 子接口（使用路由器或防火墙时）或交换虚拟接口 (SVI)（使用第 3 层交换机时）
- BGPv4，特别是用于扩展社区属性的 MP BGP 扩展（RFC 4760 和 RFC 7606）

广域网和互联网连接

交换矩阵站点的外部互联网和 WAN 连接具有大量可能的变体形式，并且这些变体形式基于底层网络设计。这些变体形式的常见相似之处表现在：边界节点通常连接到下一跳设备，并会经过该设备访问互联网和 WAN，具体取决于其路由信息。此路由基础设施可以是实际的互联网边缘路由器、WAN 边缘路由器、ISP 路由器，甚至还可以是使用多个功能的融合路由器。

关键设计注意事项在于确保此路由基础设施具有将交换矩阵站点连接到外部世界所必需的物理连接和吞吐量。

统一策略

统一策略是创建 SD-Access 解决方案背后的一个主要驱动因素。借助统一策略，有线和无线流量均在接入层（交换矩阵边缘节点）实施，且用户、设备和应用在连接网络的任何位置都具有相同的策略。

在交换矩阵站点中，通过 VXLAN GPO 报头的网段 ID（组策略 ID）和虚拟网络标识符字段来启用和传输统一策略。您可在附录 A 中找到有关此报头的其他详细信息。这样一来，可在交换矩阵站点内传输 VRF（宏）和 SGT（微）分段信息。

使用用于分布式园区的 SD-Access 时，VXLAN GPO 封装格式用于在站点之间传输数据包。这些统一策略结构存在于遍历交换矩阵站点或更大的交换矩阵域的每个数据包中。

设计具有基于 IP 的传输的交换矩阵站点时，如果分散的位置之间需要统一策略，则必须认真考虑。使用基于 IP 的传输时，交换矩阵数据包解封到本地 IP 中。这会导致策略结构丢失。

端到端宏分段

SD-Access 使用 VRF（虚拟网络或 VN）进行宏分段。VRF 为网络内的设备、接口和子网维护单独的路由和交换实例。在交换矩阵站点中，Cisco DNA Center 调配用户定义的 VRF 的配置。

交换矩阵站点之外的分段具有多种不同的变体形式，具体取决于传输类型。在用于分布式园区的 SD-Access 和 SD-WAN 传输中，虚拟网络信息在数据包内进行本地传输。

在基于 IP 的传输中，由于解封，该策略信息可能丢失。可通过两种方法使用基于 IP 的传输在交换矩阵站点之间传输虚拟网络信息。在每个交换矩阵站点之间配置 VRF Lite 逐跳选项是最简单的方法，但因为 SP 设备超出工程师的管理控制范围，这也是部署频率最低的方法。

第二种设计选项使用多协议 BGP 中的 VPNv4 地址系列传输宏分段信息。由于 BGP 是对等体之间的点对点 TCP 会话，策略结构可在每个交换矩阵站点中直接将它用作 BGP 路由基础设施之间的 IP 转发路径来遍历运营商 WAN 网络。

端到端微分段

SD-Access 使用 SGT（可扩展组标记）进行微分段。SGT 使用唯一标记形式的元数据将主机分配到组，并根据这些组应用策略。在交换矩阵重叠网络内，边缘节点和边界节点使用从 ISE 下载的 SGACL，以根据这些 SGT 做出实施决策。

交换矩阵站点之外的分段具有多种不同的变体形式，具体取决于传输类型。在用于分布式园区的 SD-Access 和 SD-WAN 传输中，虚拟网络信息在数据包内进行本地传输。

在基于 IP 的传输中，由于解封，该策略信息可能丢失。可通过两种方法使用基于 IP 的传输在交换矩阵站点之间传输 SGT 信息。在每个交换矩阵站点之间配置内联标记 (CMD) 逐跳选项是最简单的方法，但因为 SP 设备超出工程师的管理控制范围，这也是部署频率最低的方法。第二个设计选项是使用 SXP 在站点之间传输 IP 到 SGT 的绑定。使用 SXP 时，这些绑定可在站点之间通过 GRE、IPsec、DMVPN 和 GETVPN 线路传输。

SXP 具有必须予以考虑的扩展点和实施点影响。在交换矩阵站点之间，SXP 可用于在边界节点上或在北向边界的路由基础设施上实施 SGT。如果在路由基础设施上执行实施，则使用 CMD 从边界节点对 SGT 信息进行内联传输。有关部署场景、GRE 和 VPN 线路上的 SGT 的其他详细信息，以及扩展信息，请参阅 SD-Access 分段设计指南。

站点生存能力

如果 WAN 和 MAN 连接不可用，交换矩阵中的终端将无法访问跨这些线路的任何服务。对站点生存能力的需求通过平衡附加设备的相关成本和部署背后的业务驱动因素确定，同时还会将站点上受影响用户的数量考虑在内。

设计提高站点生存能力的 SD-Access 网络需要拥有位于站点本地的共享服务。当共享服务在站点本地时，需要融合路由器才能访问这些服务。

高可用性

高可用性与站点生存能力密切相关。具有单一交换矩阵边界、控制平面节点或无线控制器的站点在设备发生故障时有单点故障风险。对 SD-Access 网络的高可用性进行设计时，请务必注意，冗余设备不会增加整体规模。冗余交换矩阵边界节点和交换矩阵控制平面节点以主用-主用方式运行，WLC 作为主用-备用对运行。

交换矩阵站点参考模型

为了更好地了解常见的站点设计，对参考类别进行了简单划分。这些数字仅用作参考，不一定符合设计中所用设备的任何特定限制条件。

- **极小型站点** - 使用一体式交换矩阵覆盖一个配线柜，并通过交换机堆叠支持恢复能力；适用于终端少于 2000 个、虚拟网络少于 8 个、AP 少于 100 个的配置；边界、控制平面、边缘和无线功能在单个冗余平台上并置。

- **小型站点** - 覆盖一个办公室或楼宇；设计用于支持终端少于 10000 个、虚拟网络少于 32 个、AP 少于 200 个的配置；边界与控制平面功能在一个或两个设备上并置，单独的无线控制器具有可选的 HA 配置。
- **中型站点** - 覆盖一个具有多个配线柜的楼宇或多个楼宇；设计用于支持终端少于 25000 个、虚拟网络少于 64 个、AP 少于 1000 个的配置；使用冗余设备通过控制平面功能分布边界，单独的无线控制器具有 HA 配置。
- **大型站点** - 覆具一个具有多个配线柜的大型楼宇或多个楼宇；设计用于支持终端少于 50000 个、虚拟网络少于 64 个、AP 少于 2000 个的配置；在冗余设备上通过控制平面功能分布多个边界出口，单独的无线控制器具有 HA 配置。

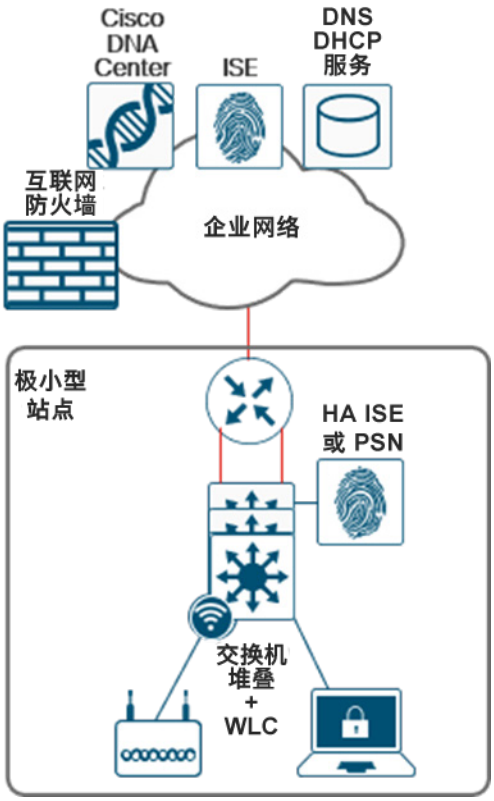
每个交换矩阵站点都包含一组支持的控制平面节点、边缘节点、边界节点和无线局域网控制器，并根据所列类别适当调整大小。ISE 策略节点还在各个站点之间分布，以满足生存能力要求。在单个物理网络中，可以部署多个交换矩阵。在这种情况下，单独的交换矩阵元素（控制平面节点、边界节点、边缘节点和 WLC）仅分配到一个交换矩阵。

在设计大小相似的站点时，请使用所提供的表格作为参考。这些数字仅用作参考，不一定符合此站点大小设计中所用设备的特定限制条件。

极小型站点 - 参考模型

极小型站点参考模型包含一个配线柜，且终端数量通常少于 2000 个。此设计的核心组件是以控制平面节点、边界节点和边缘节点这三个交换矩阵角色运行的交换机堆叠。通过这种方式部署交换机时，它称为 *一体式交换矩阵*。

图 9. 物理拓扑 - 极小型站点设计



极小型站点注意事项

由于终端数量较少，高可用性和站点生存能力不是极小型站点设计的常见要求。在所有参考设计中，DHCP、DNS、WLC 和 ISE 的本地站点服务通常都提供恢复能力和生存能力，但代价是复杂性和设备（包括一个融合路由器）数量增加。

如果在本地部署共享服务，则融合路由器通常是直接连接到一体式交换矩阵的交换机，而服务以虚拟机的形式部署到 UCS C 系列上并连接到融合路由器。另一种方法是在 WAN 路由基础设施或交换矩阵路由器中部署 UCS E 系列刀片服务器，以虚拟化共享服务。

此设计中的高可用性通过 StackWise-480（将多个物理交换机组合为一个逻辑交换机）和 StackPower（在交换机堆叠中的成员之间提供电源冗余）实现。如果使用机箱交换机，则通过冗余管理引擎和冗余电源实现高可用性。

无线局域网控制器可部署为直接连接到一体式交换矩阵的物理设备，也可部署为嵌入式 Catalyst 9800 控制器。将嵌入式 Catalyst 9800 与交换机堆叠或冗余管理引擎配合使用时，系统会自动提供 AP 和客户端 SSO。

使用交换机堆叠时，应使用来自不同堆栈成员的上游路由基础设施链路。使用机箱交换机时，应通过不同的管理引擎连接链路。要为边界节点自动切换做好准备并具备初始 IP 可访问性，通常需要在小型站点交换机和上游路由基础设施之间部署 SVI 和中继链路。

采用堆叠配置的 Catalyst 9300 系列加上嵌入式 Catalyst 9800 系列无线局域网控制器功能是适用于此设计的最佳平台。其他可用平台（例如 Catalyst 9500 系列）会增加额外的物理连接选项，但没有通过 StackWise-480 和 StackPower 获得的更强恢复能力。

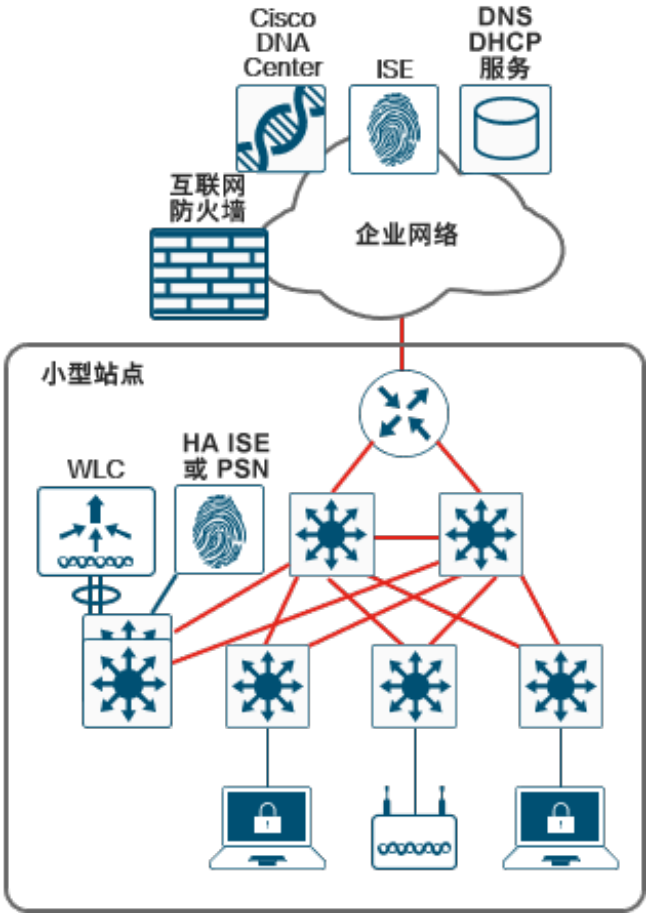
表 1. 极小型站点参考模型设计 - 指南

终端，目标数量少于	2,000
交换矩阵节点，最大数量为	1
控制平面节点，并置数量为	1
边界节点，并置数量为	1
虚拟网络，目标数量少于	8
IP 池，目标数量少于	8
无线接入点，目标数量少于	100

小型站点设计 - 参考模型

小型站点参考模型覆盖一个具有多个配线柜的楼宇或多个楼宇，且终端数量通常少于 10000 个。物理网络通常为两层，紧缩核心/分布层和接入层。

图 10. 物理拓扑 - 小型站点设计



小型站点注意事项

在小型站点中，通过在紧缩核心交换机上将边界节点和控制平面节点功能搭配使用，在交换矩阵节点中提供高可用性。要在重叠网络和底层网络中获得恢复能力和备用转发路径，紧缩核心交换机应使用交叉链路直接互相连接。

考虑到终端的数量，小型站点通常不使用 SD-Access 嵌入式无线。如果 AP 少于 200 个且客户端少于 4000 个，则嵌入式无线可以与紧缩核心交换机上的 b 并置边界节点和控制平面节点功能一起部署。

要支持更多的客户端或无线接入点，需要部署物理 WLC。要在设备中使用 HA-SSO 对或通过物理连接实现高可用性，请部署服务块。WLC 通过第 2 层端口通道连接到服务块交换机，以提供冗余接口。服务块通常是一个连接到两个紧缩核心交换机的小型交换机堆叠。如果 DHCP 和 DNS 服务器在站点本地，则此服务块可用作融合路由器。

表 2. 设计指南（限制条件可能有所不同）- 小型站点设计

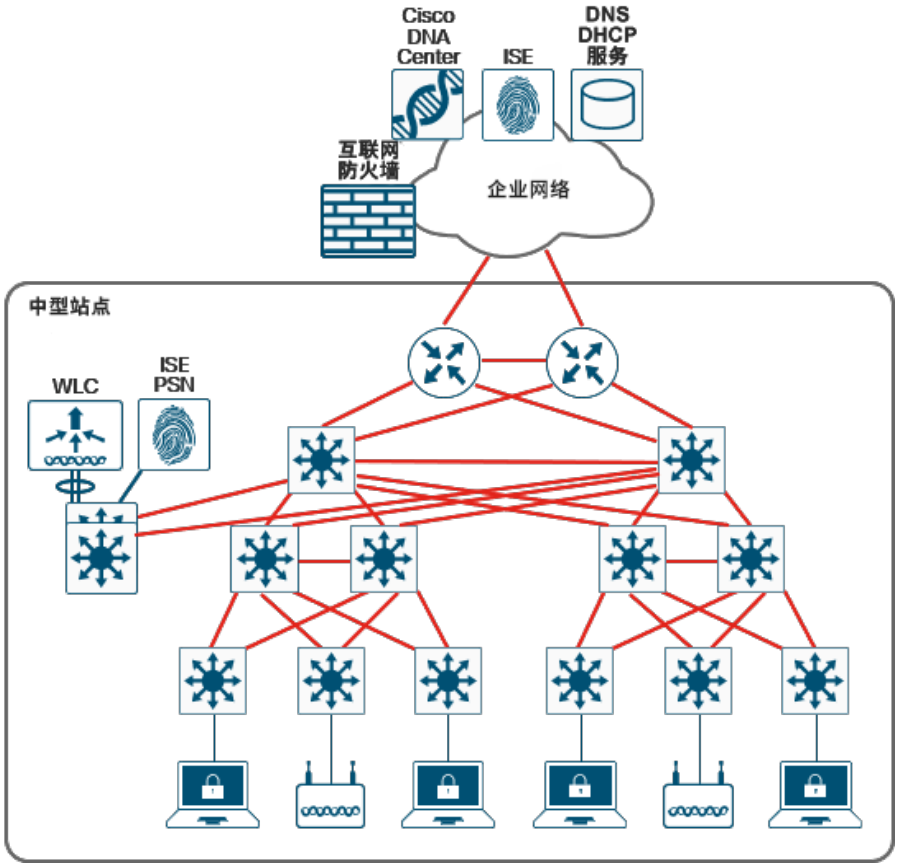
终端，目标数量少于	10,000
交换矩阵节点，最大数量为	25
控制平面节点	2
边界节点	2
虚拟网络，目标数量少于	32
IP 池，目标数量少于	100
无线接入点，目标数量少于	200

对于规模较小的部署，可以使用两层设计实施 SD-Access 交换矩阵。应该运用同样的设计原则，但无需以中间节点实施汇聚层。

中型站点设计 - 参考模型

中型站点参考模型覆盖一个具有多个配线柜的楼宇或多个楼宇，并设计为支持终端数量少于 25000 个的配置。物理网络通常为三层网络，具有核心层、分布层和接入层。它甚至可能包含一个路由器超级核心，该核心汇聚多个楼宇并充当 WAN 和互联网的网络出口点。

图 11. 物理拓扑 - 中型站点设计，三层



中型站点注意事项

在中型站点中，通过将设备专用于边界节点和控制平面节点（而不是在设备上搭配使用功能），在交换矩阵节点中实现高可用性。要在重叠网络和底层网络中获得恢复能力和备用转发路径，紧缩核心交换机应使用交叉链路直接互相连接。专用控制平面节点通常连接到站点的核心交换机。若要实现最佳转发和冗余，它们应具有通过两个核心的连接。

考虑到终端数量和分布式控制平面节点及边界节点，中型站点无法利用 SD-Access 嵌入式无线，因此已部署物理 WLC。为了实现高可用性，已部署 HA SSO 对，并通过第 2 层端口通道与服务块进行冗余物理连接。WLC 应通过其 RP 端口相互连接。服务块通常是在 VSS 或 StackWise 虚拟（连接到两个核心交换机）中运行的非模块化交换机。如果 DHCP 和 DNS 服务器在站点本地，则此服务块交换机可用作融合路由器。

表 3. 中型站点参考设计 - 指南

终端，目标数量少于	25,000
交换矩阵节点，最大数量为	250
控制平面节点 （对于 SD-Access 无线，限制为 2 + 2 个访客）	2-4
边界节点	2
虚拟网络，目标数量少于	64
IP 池，目标数量少于	300
无线接入点，目标数量少于	1,000

大型站点设计 - 参考模型

大型站点参考模型覆盖一个具有多个配线柜的楼宇或多个楼宇。物理网络通常为三层网络，具有核心层、分布层和接入层，并设计为支持终端数量少于 50000 个的配置。此网络很大，需要专用服务出口点，例如专用数据中心、共享服务块和互联网服务。大型站点注意事项

大型站点设计通常涉及多交换矩阵部署中的总部位置。企业边缘防火墙（边界防火墙）通常部署在此位置，而来自远程站点的互联网流量则通过隧道传输回此站点进行处理，然后才放入互联网中。Cisco DNA Center 和主 ISE PAN 通常部署在此位置。

控制平面节点和边界节点应是以冗余对形式部署的专用设备。专用控制平面节点应连接到每个核心交换机，以提供恢复能力和冗余转发路径。

已部署无线局域网控制器 HA SSO 对，并通过第 2 层端口通道与服务块进行冗余物理连接。WLC 应通过其 RP 端口相互连接。服务块通常是本地数据中心网络的一部分。尽管 DC 核心会连接到核心层或分布层交换机以实现可连通性，但此服务块可能位于数据中心下游相距多个跃点的位置。由于服务块和核心交换机之间有多个设备，融合路由器服务设备的位置可能会有所不同。具有适当许可证级别和功能的思科 Nexus 数据中心交换机可用于此功能。

专用内部边界节点通常用于将站点连接到数据中心核心，而专用外部边界节点则用于将站点连接到 MAN、WAN 和互联网。专用冗余路由基础设施和防火墙用于将此站点连接到外部资源，且边界节点应完全呈网状连接到这些资

源并互相连接。虽然该拓扑中所绘的边界位于园区核心，但大型站点边界通常也可与核心交换机分开，在另一个汇聚点配置。

大型站点可能包含专用的访客交换矩阵边界和控制平面节点。这些设备通常与并置交换矩阵角色（而不是分布式交换矩阵角色）一起部署，并且可物理访问并连接到 DMZ。这样可在访客和企业流量之间提供完全的控制平面和数据平面隔离，并优化要直接发送到 DMZ 的访客流量，而无需使用锚点 WLC。

表 4. 大型站点参考设计 - 指南

终端，目标数量少于	50,000
交换矩阵节点，最大数量为	1,000
控制平面节点 **（对于 SD-Access 无线，限制为 2 + 2 个访客）**	2-6
边界节点	2-4
虚拟网络，目标数量少于	64
IP 池，目标数量少于	500
无线接入点，目标数量少于	2,000

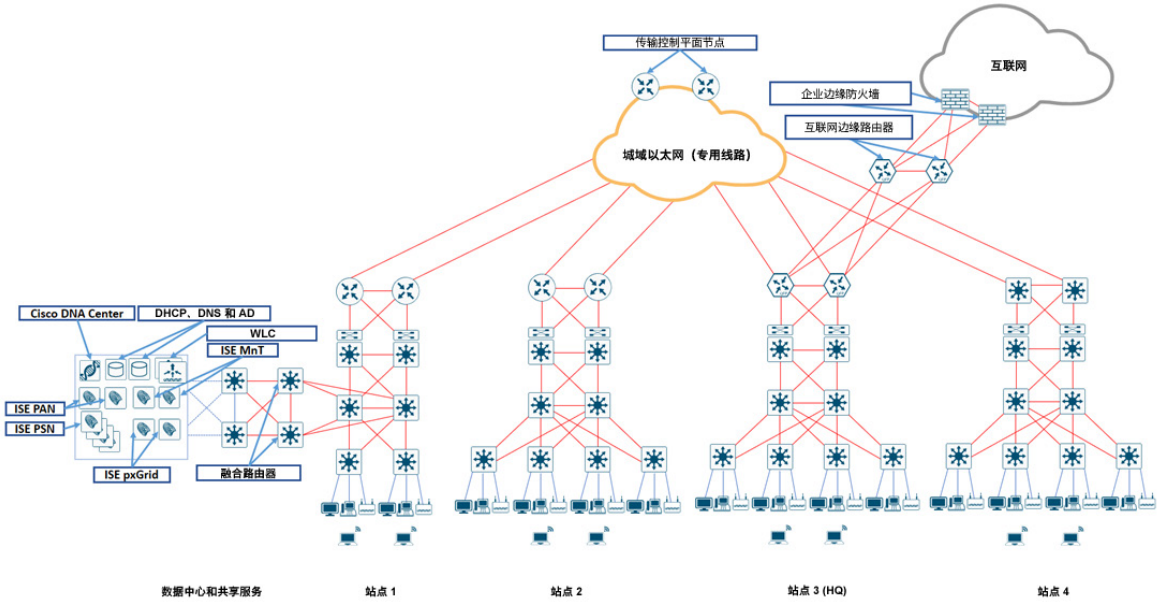
用于分布式园区的 SD-Access 设计 - 参考模型

用于分布式园区的 SD-Access 是一种城域解决方案，可将多个独立交换矩阵站点连接在一起，同时在这些站点上维护安全策略结构（VRF 和 SGT）。尽管 SD-Access 支持多站点环境和部署已有一段时间，但还没有一种自动化的简单方法来维护站点之间的策略。在每个站点的交换矩阵边界节点上，交换矩阵数据包被解封到本地 IP 中。与 SXP 结合时，可以使用本地封装在站点之间传输策略。但是，此策略配置是手动执行，强制使用 SXP 在站点之间扩展策略，并涉及 IP 到身份服务引擎内 SGT 绑定的复杂映射。

对于适用于分布式园区的 SD-Access，则不需要 SXP，这些配置是自动化的，并且复杂映射也得以简化。此解决方案通过在整个城域网络中使用一致的端到端自动化和策略来实现站点间通信。

用于分布式园区的软件定义接入使用来自 LISP 协议的控制平面信令，并将数据包保存在交换矩阵站点之间的交换矩阵 VXLAN 封装中。这将在交换矩阵站点之间分别维护 VRF 和 SGT 的宏分段和微分段策略结构。数据包的原始以太网报头会被保留，用来启用 SD-Access 无线的第 2 层重叠网络服务。结果是网络的地址不可知，因为策略是通过组成员身份维护的。

图 12. 物理拓扑 - 用于分布式园区的 SD-Access



分布式园区注意事项

支持分布式园区解决方案的核心组件是 SD-Access 传输网络和传输控制平面节点。这两个都是本解决方案引入的新架构构件。SD-Access 传输网络只是同一城市、城域内或大型企业园区的楼宇之间的物理城域连接。

SD-Access 传输

SD-Access 传输用于适用于分布式园区的 SD-Access。对于使用 SD-Access 传输网络的分布式园区设计，关键的考虑因素是，应使用类似园区的连接建立交换矩阵站点之间和连接 Cisco DNA Center 的网络。这些连接应该是高带宽（以太网完全端口速度，不含子速率服务），低延迟（一般指导原则为低于 10 ms），并且应适应在园区网络中用于 SD-Access 的 MTU 设置（通常为 9100 字节）。物理连接可以是支持类似带宽、端口速率、延迟和 MTU 连接能力的直接光纤连接、租用暗光纤、基于 WDM 系统波长的以太网或城域以太网系统（VPLS 等）。使用 SD-Access 传输时，使用交换矩阵 VXLAN 封装在站点之间封装数据包。

传输控制平面节点

传输控制平面节点跟踪交换矩阵域的所有汇聚路由，并将这些路由关联到交换矩阵站点。当来自一个站点中的终端的流量需要将流量发送到另一个站点中的终端时，系统会查询传输控制平面节点以确定应将此流量发送到哪个站点的边界节点。传输控制平面节点的作用是了解哪些前缀与每个交换矩阵站点关联，并使用控制平面信令在 SD-Access 传输网络中将流量定向到这些站点。

传输控制平面部署位置

传输控制平面节点实体不必部署于传输区域（站点之间的城域连接）中，也不需要专用于自己的交换矩阵站点，但常见拓扑文档通常会这样描述它们。这些设备通常部署在各自的专用位置，仅可通过 SD-Access 传输城域网络进行访问，但这并不是必需的。

虽然仅可通过传输区域访问，但这些路由器不充当数据包转发路径中的物理传输跃点。它们的工作方式与 DNS 服务器类似，因为它们会被用来查询信息，即使数据包不通过它们传输。这是一个重要注意事项。

主要注意事项

站点之间的传输网络最典型也最常用的部署是采用基于城域以太网系统的直连或租用光纤。虽然城域以太网有若干不同种类（VPLS、VPWS 等），但每个站点的边缘路由器和交换机最终通过内部网关路由 (IGP) 协议交换底层路由。在 SD-Access 中，这通常使用 IS-IS 路由协议完成，但也支持其他 IGP。

交换矩阵站点之间必须存在 IP 可访问性。具体而言，在所有交换矩阵节点上的环回 0 接口之间必须有一个已知的底层网络路由。传输控制平面节点上的现有 BGP 配置和对等体可能与 Cisco DNA Center 调配的配置有复杂的交互，应避免使用。BGP 专有编号 AS 65540 被保留用于传输控制平面节点，并由 Cisco DNA Center 自动调配。在被发现或调配之前，传输控制平面节点应具有通过 IGP 连接交换矩阵站点的 IP 可访问性。

建议不要遍历站点之间的数据转发路径中的传输控制平面节点。传输控制平面节点应始终部署为一对设备，以提供恢复能力和高可用性。

平台角色和功能注意事项

请考虑推荐的功能角色，根据网络所需容量和功能选择您的 SD-Access 网络平台。在本指南开发过程中测试的角色已在相关部署指南中注明，网址为：https://www.cisco.com/go/cvd/campus。

有关每个版本的思科 SD-Access 支持的平台和软件的最新信息，请参阅 SD-Access 硬件和软件兼容性表。您的物理网络设计要求推动平台和软件的选择。在 SD-Access 部署中需要考虑的平台功能：

- 支持各种思科 Catalyst 9000 系列设备（有线和无线）以及 Catalyst 3850 和 3650；但是，仅特定设备作为交换矩阵边缘、边界和控制平面节点角色受到支持，且可用角色可能随新版本的 Cisco DNA Center 和思科 IOS XE 软件的发布而扩展。
- 还支持思科 Catalyst 4500 和 6800 系列以及思科 Nexus 7700 系列等其他设备，但可能有特定的管理引擎模块、线卡模块和面向交换矩阵的接口要求。此外，角色可能会减少。例如，Nexus 7700 软件可能会将 SD-Access 角色限制为仅用作外部边界，并且还需要单独的控制平面节点。
- 以控制平面和边界节点的形式支持各种路由平台，例如思科 ISR 4400 和 4300 系列集成多业务路由器、思科 ASR 1000-X 和 1000-HX 系列聚合多服务路由器，但它们不能是交换矩阵边缘节点。此外，还支持思科云服务路由器 1000V 系列，但仅作为控制平面节点受到支持。
- 思科 Catalyst 9800（独立和嵌入式）、8540、5520 和 3504 系列无线局域网控制器对其支持有特定的软件要求。同样，思科 Catalyst 9100 和思科 Aironet 第二代和第一代 AP 要求提供特定软件版本。
- 必须使用与 Cisco DNA Center 兼容的版本部署思科 ISE。

迁移到 SD-Access

通过添加基础设施组件，将其互联，并使用具有思科即插即用功能的 Cisco DNA Center 从头开始自动调配网络架构，就可以轻而易举地创建 SD-Access 全新环境网络。迁移现有网络则需要进行更多规划。以下是一些注意事项:

- 迁移通常意味着使用手动创建的底层。组织的底层网络是否已经包括 “底层网络” 部分所述的元素？或者，您是否必须将网络重新配置为第 3 层接入模型？
- 网络中的 SD-Access 组件是否支持目标拓扑所需的规模？或者是否需要以其他平台扩充硬件和软件平台？
- 组织是否已为 IP 寻址和 DHCP 作用域管理的更改做好准备？
- 如果您计划启用多个重叠网络，将这些重叠网络与常用服务（例如：互联网、DNS/DHCP、数据中心应用）集成的战略是什么？
- 是否已经实施 SGT？策略实施点在哪里？如果在交换矩阵内使用 SGT 和多个重叠网络进行分段和虚拟化，将其扩展到交换矩阵外的要求是什么？是否具备必要的基础设施，可以支持思科 TrustSec、VRF-Lite、MPLS、融合路由器或者扩展和支持分段及虚拟化所需的其他技术？
- 漫游域内的无线覆盖能否在某个时间点升级？或者您是否需要依靠采用机顶盒设备的战略？

将现有网络迁移到 SD-Access 时，主要有两种方法。如果要更换许多现有平台，而且有充足的功率、空间和冷却能力，则选择构建并行 SD-Access 网络可以方便用户转换。构建与现有网络集成的并行网络实际上是构建全新环境网络的变化形式。另一种方法是将接入交换机增量迁移到 SD-Access 交换矩阵中。这种战略适用于已经安装了能够支持 SD-Access 的设备或存在环境限制的网络。

为了帮助进行网络迁移，SD-Access 支持第 2 层边界结构，可在过渡阶段临时使用。使用连接到现有传统第 2 层接入网络的一个边界节点（其中现有的第 2 层接入 VLAN 映射到 SD-Access 重叠网络中）创建第 2 层边界切换。您可以使用 EtherChannel 在一个第 2 层边界和现有的外部第 2 层接入网络之间创建链路冗余。现有外部第 2 层接入网络上的机箱冗余可以使用 StackWise 交换机堆叠、虚拟交换系统或 StackWise 虚拟配置。第 2 层边界上支持的主机数量因 SD-Access 版本而异，最早版本限制为 4000 个主机。将交换矩阵 DHCP 服务规划为支持交换矩阵终端以及在连接时迁移非交换矩阵第 2 层网络设备。

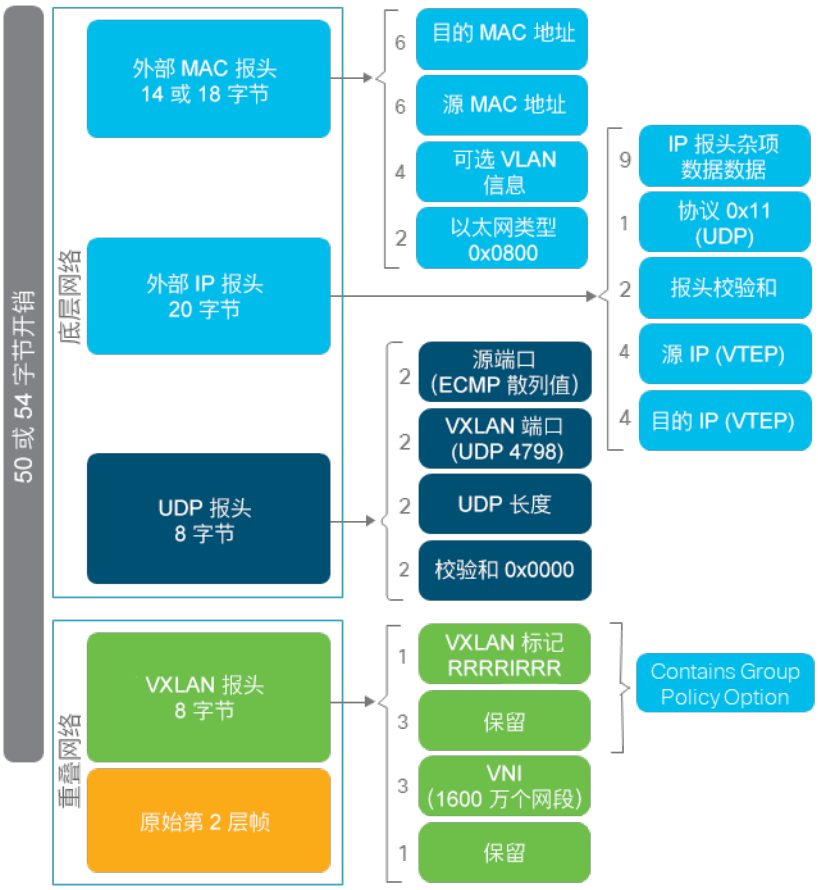
有关迁移主题的详细介绍，请参阅 Cisco.com 上的软件定义的接入迁移。

附录 A - SD-Access 交换矩阵协议

交换矩阵数据平面

RFC 7348 将虚拟可扩展局域网 (VXLAN) 定义为在第 3 层网络上重叠第 2 层网络的一种方式。借助 VXLAN，可以使用 UDP/IP 在第 3 层网络上标记原始第 2 层帧。每个重叠网络称为 VXLAN 网段，并使用 24 位 VXLAN 虚拟网络标识符来标识，最多支持 1600 万个 VXLAN 网段。

图 13. RFC 7348 VXLAN 报头



SD-Access 交换矩阵使用 VXLAN 数据平面传输完整的原始第 2 层帧，并另行使用定位/ID 分离协议作为控制平面来解析终端到位置的映射。SD-Access 交换矩阵使用 https://tools.ietf.org/html/draft-smith-vxlan-group-policy-05 中所述的经过修改的 VXLAN GPO 格式，替换 VXLAN 报头中的 16 个保留位，以传输最多 64000 个 SGT。

第 3 层重叠网络的 VNI 映射到虚拟路由和转发实例，而第 2 层 VNI 则映射到 VLAN 广播域，二者均可为每个虚拟网络提供隔离数据和控制平面的机制。SGT 传输用户的组成员身份信息，并在虚拟网络内部提供数据平面分段。

交换矩阵控制平面

RFC 6830 和其他 RFC 将 LISP 定义为网络架构和一组协议，用于实施进行 IP 寻址和转发的新语义。在传统 IP 网络中，使用 IP 地址将终端及其物理位置标识为路由器上分配的子网的一部分。在启用 LISP 的网络中，一个 IP 地址或 MAC 地址用作设备的终端标识符，另一个 IP 地址用作 RLOC，用于表示该设备的物理位置（通常是 EID 连接到的路由器的环回地址）。EID 和 RLOC 相组合，即可为流量转发提供必要的信息。RLOC 地址是底层路由域的一部分，而且 EID 可以独立分配，不必与位置相关。

LISP 架构需要一个映射系统来存储 EID 并将其解析为 RLOC。这类似于使用 DNS 解析主机名的 IP 地址。EID 前缀（带有 /32 “主机” 掩码的 IPv4 地址或 MAC 地址）连同其关联的 RLOC 一起注册到映射服务器中。向 EID 发送流量时，源 RLOC 查询映射系统以确定流量封装的目的 RLOC。与 DNS 一样，本地节点可能没有网络中所有内容的相关信息，而是仅在本地主机需要它进行通信（拉取模型）时才要求提供信息，然后缓存信息以提高效率。

虽然在 SD-Access 中部署交换矩阵并不需要全面了解 LISP 和 VXLAN，但是了解这些技术如何支持部署目标却非常有帮助。LISP 架构提供的优势包括:

- **网络虚拟化** – 使用 LISP 实例 ID 保持独立的 VRF 拓扑。从数据平面的角度来看，LISP 实例 ID 映射到 VNI。
- **子网扩展** – 可以扩展单个子网，使其存在于多个 RLOC。EID 与 RLOC 分开，因此可以跨不同的 RLOC 扩展子网。LISP 架构中的 RLOC 用于在第 3 层网络上封装 EID 流量。由于能够用作跨多个 RLOC 的任播网关，EID 客户端配置（IP 地址、子网和网关）可以保持不变，即便当客户端跨扩展子网移到不同的物理连接点时也是如此。
- **路由表缩小** – 只有 RLOC 需要在全局路由表中可接通。本地 EID 缓存在本地节点上，而远程 EID 则通过会话学习获知。会话学习过程只在转发表中填充通过该节点通信的终端。借助此功能可以高效利用转发表。

附录 B – 术语表

AAA 身份验证、授权和记账

ACL 访问控制列表

AP 无线接入点

BGP 边界网关协议

CAPWAP 无线接入点控制和调配协议

Cisco DNA 思科全数字化网络架构

CMD 思科元数据

DMZ 防火墙隔离区

EID 终端标识符

HTDB 主机跟踪数据库

IGP 内部网关协议

ISE 思科身份服务引擎

LISP 定位/ID 分离协议

MR 映射解析器

MS 映射服务器

MTU 最大传输单位

RLOC 路由定位器

SD-Access 软件定义接入

SGACL 可扩展组访问控制列表

SGT 可扩展组标记

SXP 可扩展组标记交换协议

VLAN 虚拟局域网

VN 虚拟网络

VNI 虚拟可扩展局域网网络标识符

VRF 虚拟路由和转发

VXLAN 虚拟可扩展局域网

反馈

若对本指南和相关指南有任何意见和建议，可以在 https://cs.co/en-cvds 上的思科社区中参与讨论。

美洲总部
Cisco Systems, Inc.
加州圣何西

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。