思科验证设计

软件定义的接入设计指南

2017 年 8 月

目录

思科全数字化网络架构和软件定义的接入简介

思科® 全数字化网络架构 (Cisco DNA) 不仅提供了实现全数字化的路线图，而且为立竿见影地实现网络自动化、网络保证和网络安全的优势提供了途径。思科软件定义的接入 (SD-Access) 架构是从传统园区局域网设计演变而来的 Cisco DNA。SD-Access 使用 Cisco DNA 中心来设计和调配智能网络，对其应用策略，并为其提供园区有线和无线网络保证。园区交换矩阵技术作为 SD-Access 不可或缺的组成部分，引入了可编程的重叠，能够跨有线和无线园区实现易于部署的网络虚拟化。除网络虚拟化以外，园区交换矩阵技术还可以根据用户身份和组成员身份提供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的组来提供微分段功能。使用 Cisco DNA 中心自动创建虚拟网络可减少运营费用，同时还可提供以下优势：通过集成的安全功能降低风险；通过保证和分析功能提高网络性能。

本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。本指南是相关的 SD-Access 部署指南的配套文档，该部署指南则提供了实施本指南中所述设计所需的配置。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。

如需相关的设计指南、部署指南和白皮书，请参阅以下页面：http://www.cisco.com/go/designzone

全数字化组织的网络要求

随着全数字化的发展，软件应用正在从单纯地支持业务流程演变为在某些情况下成为主要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，既需要扩展网络容量以迅速应对应用需求，又需要为应用发展提供支持。因为园区局域网是位于某个位置的用户和设备在访问应用时所要通过的网络，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。

以下是有助于推动现有园区网络发展的关键要求。

为发展和扩展提供灵活的以太网基础

- **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（随思科通用型以太网供电提供）的以太网供电，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 PoE 永久电源。思科 Catalyst 9000 系列接入层交换机支持永久 PoE，并支持未来将会面市的每端口 100W 技术。
- **增加带宽需求** – 在网络的整个生命周期内，带宽需求会翻上一倍甚至多倍，导致新网络需要做好汇聚的准备，随着时间的推移，使用的容量从 10 Gbps 以太网增加到 40 Gbps 再到 100 Gbps。
- **简化部署和自动化** – 使用开放式 API 通过集中式控制器进行网络设备的配置和管理，可以利用 UI 和现有协调系统以非常快的速度和更低的风险部署网络设备和服务。

集成网络安全

- **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。
- **网络保证和分析** – 利用遥感勘测提高网络、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，甚至预测加密流量中存在的风险。
- **身份服务** – 标识连接到网络的用户和设备的身份，使用可扩展的组成员身份并将设备映射到虚拟网络 (VN) 中，为实施用于进行访问控制和网络分段的安全策略提供所需的情景信息。
- **基于组的策略** – 根据用户组信息创建安全策略，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 (SGT)（也称为*安全组标记*）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和控制平面相互隔离的多个 VN，从而提供多租户支持和安全防护。

软件定义的接入架构

园区交换矩阵技术支持 SD-Access 架构，因此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），以便创建替代拓扑来连接设备。重叠网络通常用于在数据中心交换矩阵（例如：ACI、VXLAN 和 FabricPath）中通过虚拟机移动性提供第 2 层和第 3 层逻辑网络。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。有关 SD-Access 设计的建议将在“设计注意事项”部分介绍。

底层网络

底层网络由属于 SD-Access 网络一部分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。理论上，任何拓扑和路由协议都可以使用，但强烈建议在园区边缘实施精心设计的第 3 层基础，以确保网络的性能、可扩展性和高可用性。在 SD-Access 架构中，终端用户子网并非底层网络的一部分。

技术提示

Cisco DNA 中心可以使用思科网络即插即用自动完成底层网络的部署。

技术提示

SD-Access 1.0 解决方案支持 IPv4 底层网络。有关 IPv6 底层网络，请参阅您的软件版本的相应版本说明以确认是否支持。

重叠网络

重叠网络在底层网络上运行，以便创建虚拟网络。数据平面流量和控制平面行为都控制在每个虚拟网络内部，除了与底层网络隔离之外，各虚拟网络之间也保持隔离。在 SD-Access 交换矩阵中，通过封装以交换矩阵边界为起止点的 IP 隧道上的用户流量来实施虚拟化。使用 VRF-Lite 和 MPLS VPN 等传统虚拟化技术保留扩展到交换矩阵外部的网络虚拟化。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。

在重叠网络中的交换矩阵边界和交换矩阵边缘节点，使用 LISP 头端复制提供 IPv4 组播转发。您需要将边界节点的 PIM 路由与位于交换矩阵外部的相邻组播路由器集成。Cisco DNA 中心将配置 PIM、IGMP 和 LISP 组播支持。

技术提示

SD-Access 1.0 解决方案既支持 PIM SM 也支持 PIM SSM。

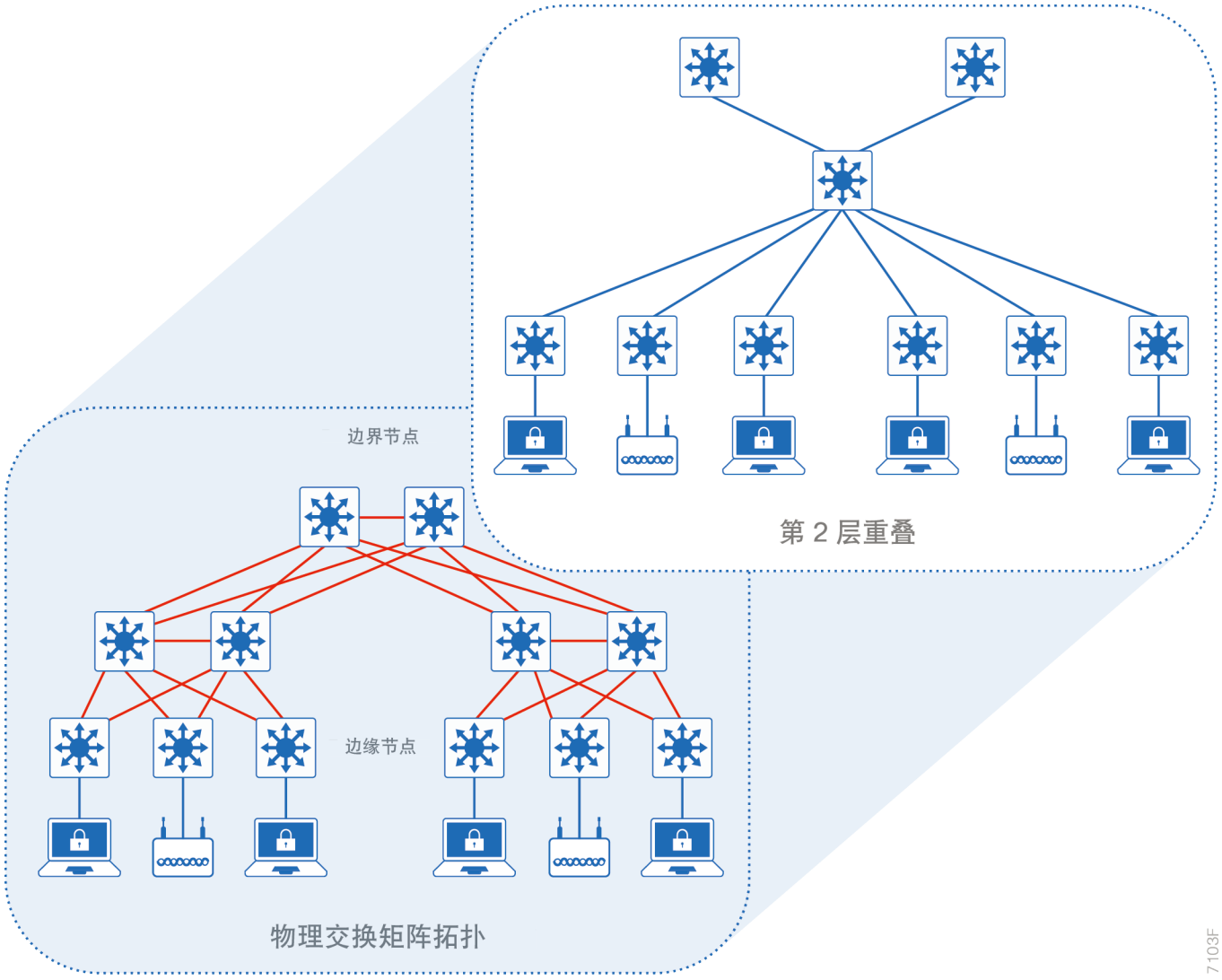
第 2 层重叠

第 2 层重叠模拟局域网网段来传输 IP 和非 IP 帧。第 2 层重叠在第 3 层底层上负载单个子网。第 2 层重叠可用于模拟物理拓扑，并发送第 2 层泛洪。

技术提示

SD-Access 1.0 解决方案支持在第 2 层重叠中仅传输 IP 帧，不发送第 2 层泛洪。有关非 IP 帧的传输和第 2 层泛洪，请参阅您的软件版本的相应版本说明以确认是否支持。

图 1　第 2 层重叠 - 逻辑交换连接



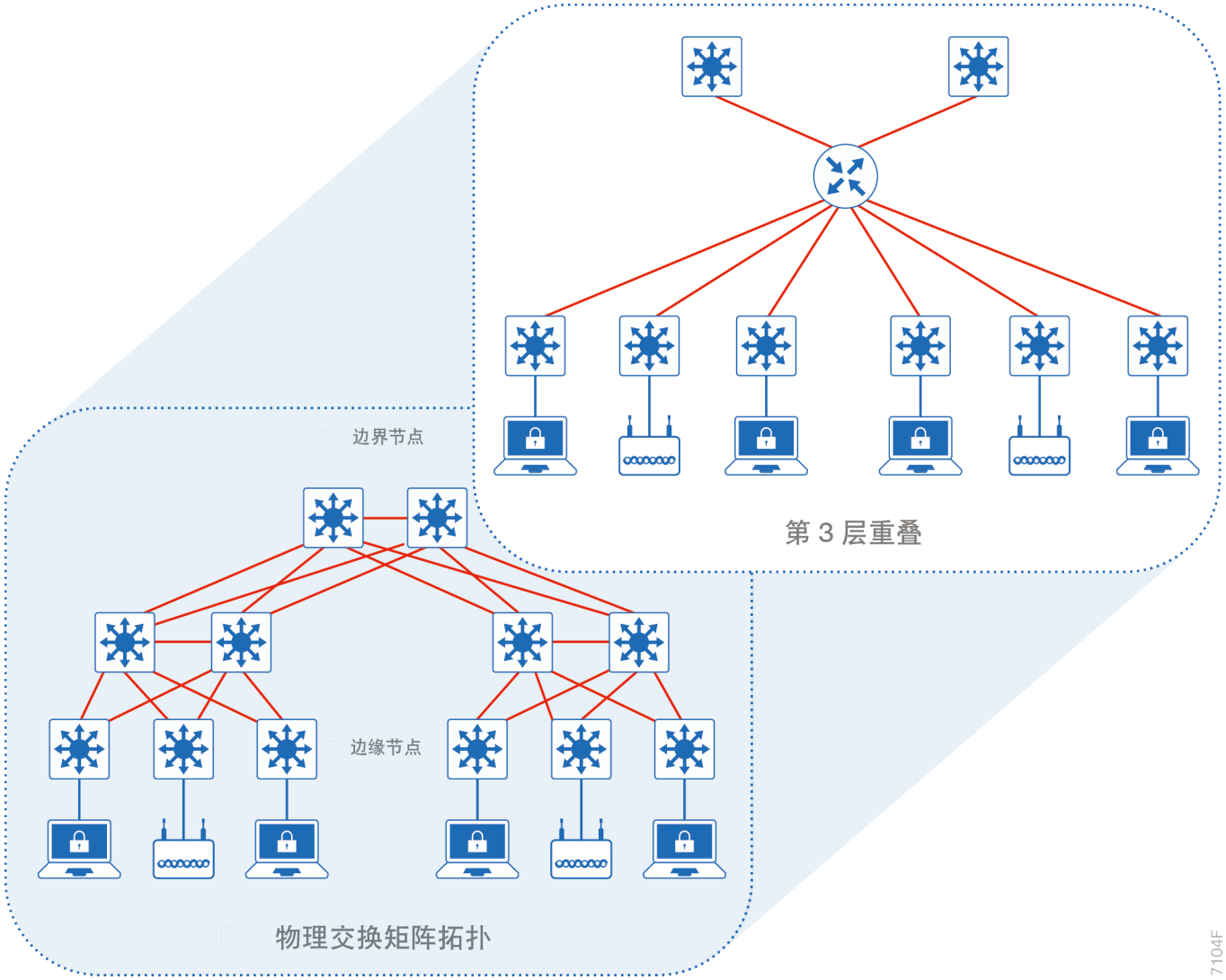
第 3 层重叠

第 3 层重叠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。支持跨不同的第 3 层重叠将 IP 地址空间重叠，只要在交换矩阵外部使用 VRF-Lite 和 MPLS L3VPN 等现有网络虚拟化功能保留网络虚拟化。

技术提示

SD-Access 1.0 解决方案支持 IPv4 重叠。对于同一 WLC 上的无线客户端，不支持重叠 IP。有关 IPv6 重叠，请参阅您的软件版本的相应版本说明以确认是否支持。

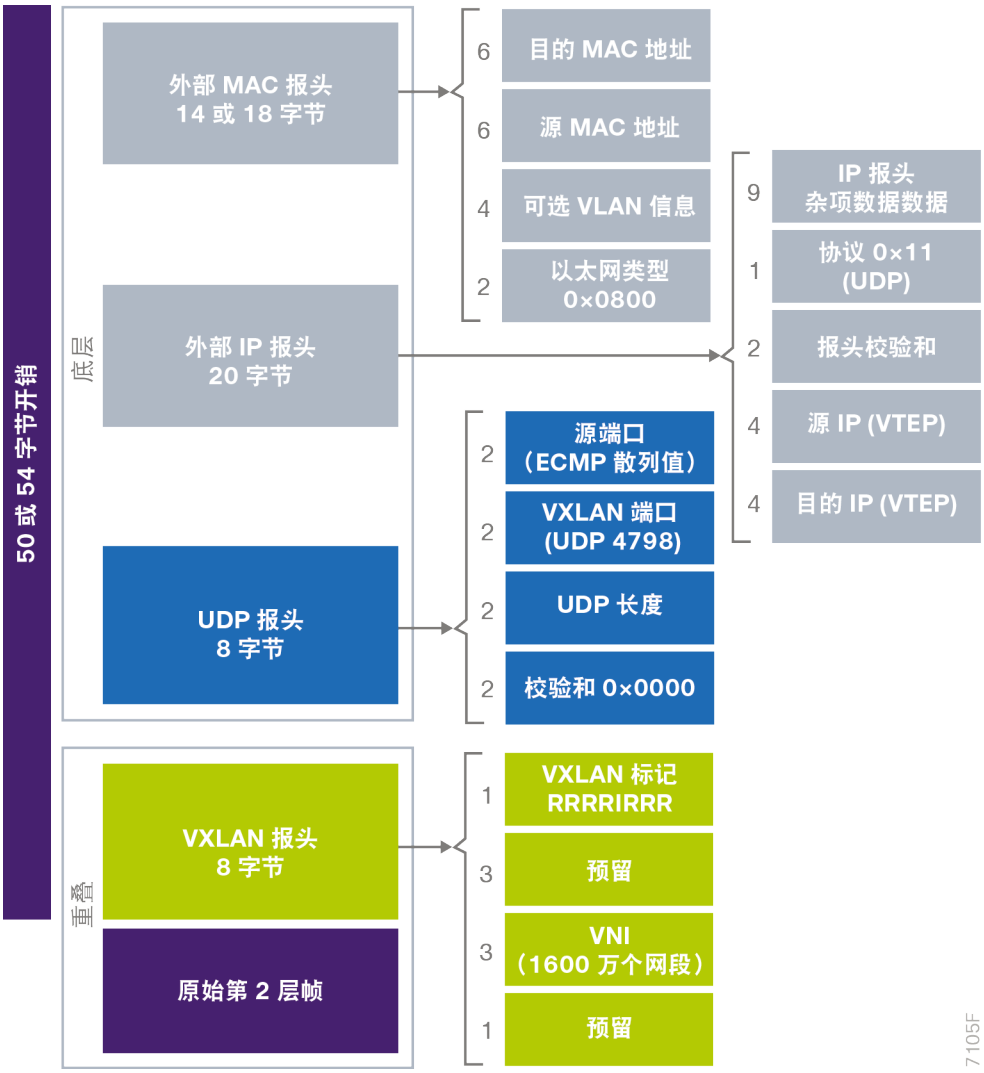
图 2　第 3 层重叠 - 逻辑路由连接



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 层网络上隧道传输原始第 2 层帧。每个节点的隧道接口称为 VXLAN 隧道终端 (VTEP)。VTEP 依靠数据平面学习（或依靠控制平面）为流量封装确定远程终端到 VTEP 的映射。每个重叠网络称为 VXLAN 网段，并使用最多可支持 1600 万个 VXLAN 网段的 24 位 VXLAN 网络标识符 (VNI) 来标识。

图 3　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 (LISP) 作为控制平面来解析终端到 VTEP 的映射。SD-Access 交换矩阵替换 VXLAN 报头中的 16 个保留位，以便传输最多 64,000 个 SGT。

第 3 层重叠的 VNI 映射到虚拟路由和转发 (VRF) 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 地址用作设备的终端标识符 (EID)，另一个 IP 地址用作路由定位器 (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。

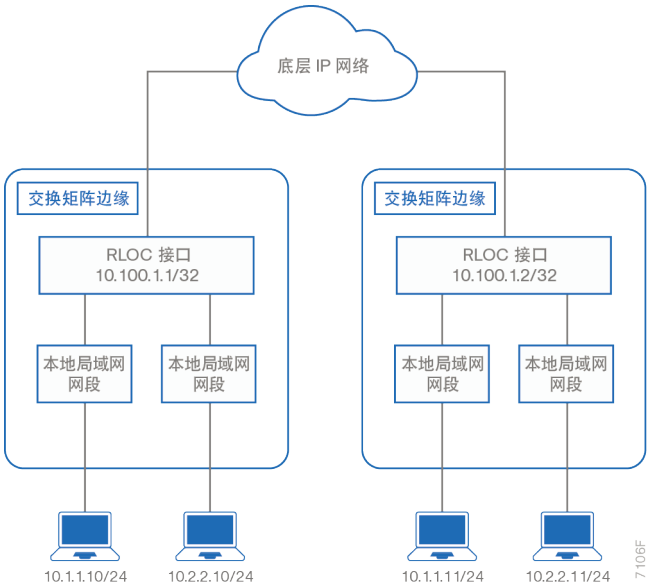
LISP 架构需要一个映射系统来存储 EID 并将其解析为 RLOC。这类似于使用 DNS 解析主机名的 IP 地址，也类似于前面提到的 VXLAN 数据平面中的 VTEP 映射。EID 前缀（带有 /32“主机”掩码的 IPv4 地址或 MAC 地址）连同其关联的 RLOC 一起注册到映射服务器中。向 EID 发送流量时，源 RLOC 查询映射系统以确定流量封装的目的 RLOC。

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 相当于 VXLAN 中的 VTEP 功能，因为它是用于在第 3 层网络中封装 EID 流量的入口和出口隧道。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达。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。

在下图所示的例子中，两个子网属于重叠网络的一部分并且跨物理上独立的路由器扩展。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 4　LISP 拓扑示例



无线集成

SD-Access 支持传统思科统一无线网络 (CUWN) 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。或者，您也可以使用另外两个组件（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。交换矩阵控制器是受支持的思科无线局域网控制器 (WLC)，它配置为与交换矩阵 LISP 控制平面通信，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现有思科第二代和第一代 802.11ac 技术 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。

技术提示

有关第二代和第一代 AP 在功能支持方面的差异，请参阅您的软件版本的相应版本说明。

技术提示

SD-Access 1.0 解决方案适用的 Cisco DNA 中心支持自动实现交换矩阵无线功能。要确认是否支持非交换矩阵工作模式，请参阅您的软件版本的相应版本说明。

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流量无需进行 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。流量将直接转发到 VTEP，通过 SD-Access 交换矩阵采取最佳路径传输到目的，并且无论有线还是无线终端连接都使用一致的策略。通过在 DMZ 网段部署访客交换矩阵边界节点，对访客用户使用专用 VN 将其隔离，可以实现对无线访客的支持。Cisco DNA 中心可自动完成管理实施完整访客解决方案的工作流程。

AP 的 SD-Access 无线控制平面使用通往 WLC 的 CAPWAP 隧道，类似于传统的 CUWN 控制平面。不过，WLC 与 SD-Access LISP 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。LISP 控制平面本身就支持漫游功能，如果与新 RLOC 关联的无线客户端 EID 发生任何更改，它都会相应更新其主机跟踪数据库。

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 隧道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。

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，以及基于策略一致性的端到端分段。无线集成还能让 WLC 摆脱数据平面转发职责，而继续用作无线域的集中式服务和控制平面。

解决方案管理

如前所述，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 中心（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 中心还如“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）。

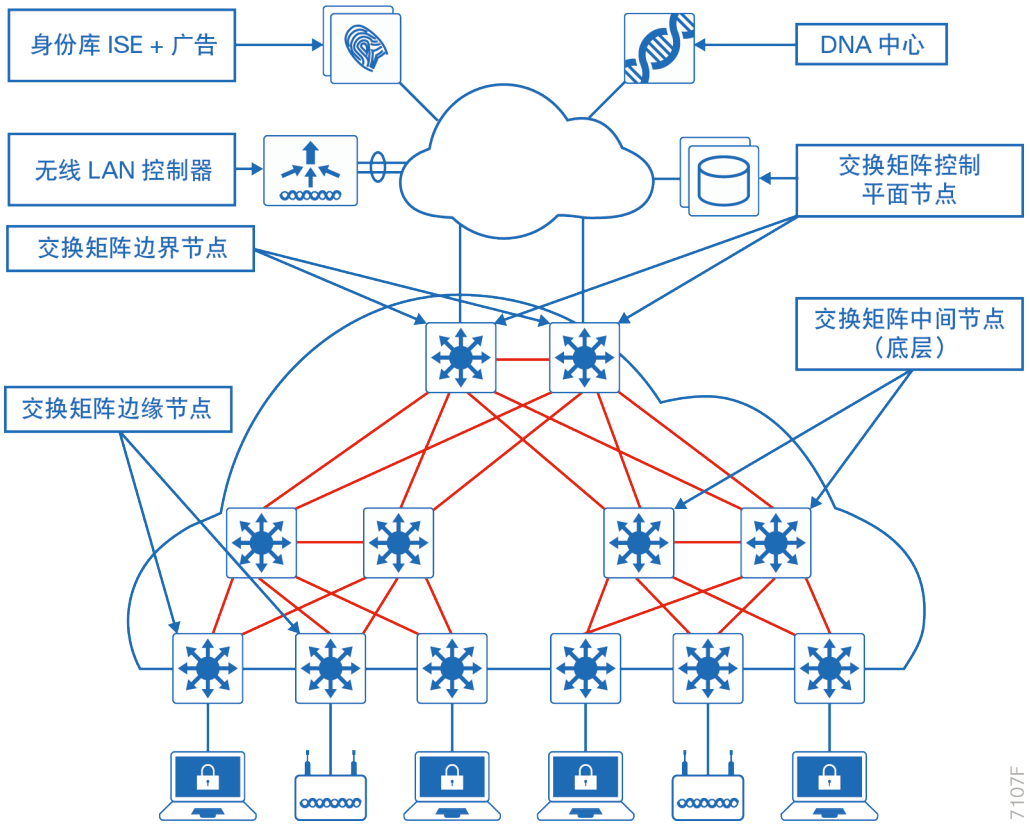
总而言之，Cisco DNA 中心是 SD-Access 不可或缺的一部分，可以将设备自动部署到网络中，提供确保运营效率所需的速度和一致性。组织在部署和维护网络时，则可获益于减少的成本和降低的风险。

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 SD-Access 控制器相结合，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。

解决方案组件

SD-Access 解决方案将 Cisco DNA 中心企业控制器、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，交换矩阵由交换矩阵控制平面节点、边缘节点、中间节点和边界节点组成。无线集成使其增加了交换矩阵 WLC 和交换矩阵模式 AP 组件。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 5　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。控制平面节点功能在边界节点或专用节点上实例化。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 用于从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** - 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，用于通知检测到的终端的控制平面节点，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，可将该终端放入虚拟网络。可以使用 802.1X，以静态或动态方式将终端映射到 VLAN 中。或者，也可以通过分配 SGT 在交换矩阵边缘提供分段和策略实施。
- **任播第 3 层网关** - 在每个节点使用共享同一个 EID 子网的通用网关（IP 和 MAC 地址）可以跨不同 RLOC 实现最佳转发和移动。
- **LISP 转发** - 交换矩阵边缘节点并非使用常用的基于路由的决定，而是查询映射服务器来确定与目的 IP 关联的 RLOC，并使用该信息在 VXLAN 中封装流量。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 CEF 表并安装到硬件中。如果在交换矩阵边缘收到未本地连接的终端的 VXLAN 封装流量，则会向发送方交换矩阵边缘发送 LISP 请求映射请求，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。

中间节点

交换矩阵中间节点是第 3 层网络的一部分，将边缘节点与边界节点互联。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。中间节点仅在交换矩阵内部路由 IP 流量。对于中间节点，没有 VXLAN 封装/解封或 LISP 控制平面消息方面的要求，只有一个额外要求，即能够承受包含嵌入式 VXLAN 信息的 IP 数据包额外附加的大小。

边界节点

交换矩阵边界节点用作 SD-Access 交换矩阵域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。交换矩阵边界节点可配置为特定网络地址（例如广域网网络）的网关，也可配置为可用于互联网的默认边界角色或交换矩阵的通用退出点。边界节点实施以下功能：

- **通告 EID 子网** - 交换矩阵边界运行内部网关协议 (IGP) 或边界网关协议 (BGP) 作为路由协议，以便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发往 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节点来访问 EID 信息。
- **交换矩阵域退出点** - 默认交换矩阵边界是交换矩阵边缘节点的默认网关。此退出点使用 LISP 代理隧道路由器功能实施。此退出点也可以是连接到网络的非默认交换矩阵边界，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。使用内联标记功能时，该节点会将 VXLAN 报头中的标记映射为思科元数据 (CMD)，或者也可以通过 SGT 交换协议 (SXP) 传输该标记，从而与思科 TrustSec 解决方案无缝集成。

交换矩阵无线局域网控制器

交换矩阵 WLC 将用于无线的控制平面集成到交换矩阵控制平面中。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 由交换矩阵模式 AP 通过交换矩阵为其直接转发流量。

交换矩阵模式 AP

交换矩阵模式 AP 是与交换矩阵 WLC 关联的思科第二代和第一代 802.11ac 技术 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 802.11AC 无线介质服务，应用 AVC、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 AP 作为本地模式 AP 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。

当无线客户端连接到交换矩阵模式 AP 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 VNID 和 ISE 提供的 SGT 更新交换矩阵模式 AP，然后代表交换矩阵边缘节点交换机将无线客户端第 2 层 EID 代理注册到 LISP 控制平面中。建立初始连接后，在该 AP 使用第 2 层 VNI 信息对无线客户端通信进行 VXLAN 封装，发往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 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。通过在 ISE 上使用思科平台交换架构 (pxGrid) 和 RESTful 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 SD-Access 控制器集成。

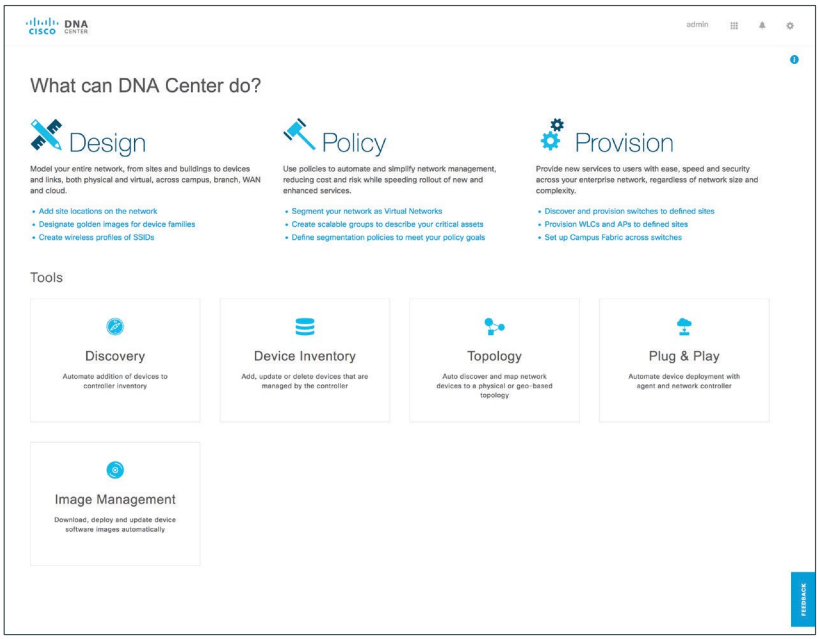
SD-Access 解决方案通过以下方式集成思科 TrustSec：对基于组的策略提供端到端支持，包括数据平面流量的 VXLAN 报头中的 SGT 信息，同时采用分配唯一 VNI 的方法支持多个 VN。组、策略、身份验证、授权和记账 (AAA) 服务及终端分析由 ISE 驱动并通过 Cisco DNA 中心的策略编写工作流程进行协调。

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 集中创建和管理。ISE 和 Cisco DNA 中心通过 RESTful API 紧密集成，策略的管理由 Cisco DNA 中心驱动。

Cisco DNA 中心

SD-Access 解决方案的自动化功能以 Cisco DNA 中心为核心。Cisco DNA 中心是在应用策略基础设施控制器企业模块 (APIC-EM) 上运行的应用，使用控制器提供的服务进行规划、准备、安装和集成。

图 6 Cisco DNA 中心控制面板



Cisco DNA 中心对工作流程的四个主要方面进行集中管理。

- **设计** - 配置设备全局设置、物理设备清单的网站配置文件、DNS、DHCP、IP 寻址、软件映像管理、即插即用和用户访问。
- **策略** - 定义业务目标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，以及为组定义策略合同。
- **调配** - 调配设备以进行管理，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、CUWN 无线和外部连接。
- **保证** - 启用运行状况得分控制面板、客户端/设备 360° 视图、节点、客户端和路径跟踪。

Cisco DNA 中心支持通过开放式 API 实现集成。例如，可以通过 Cisco DNA 中心将 Infoblox IP 地址管理和策略实施与 ISE 集成。一组全面的北向 RESTful 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 RESTful 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 RESTful 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，提供确保运营效率所需的速度和一致性，Cisco DNA 中心是关键。使用 Cisco DNA 中心的组织在部署和维护网络时，则可获益于减少的成本和降低的风险。

SD-Access 设计注意事项

SD-Access 交换矩阵的设计并非一种设计适合所有情况的万全之策。交换矩阵的规模可以小到只是一个接入层-分布层块，也可以有三层园区部署这么大。在一个网络中可以部署多个交换矩阵，只要交换矩阵的元素只分配给单个交换矩阵。

平台角色和建议

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。

技术提示

要实现所示功能，必须满足最低软件版本要求。有些平台即便包含相应功能，也未列作特定角色的推荐平台。有关详细信息，请参阅您的平台的软件版本说明；有关测试用代码版本，请参阅 CVD 部署指南。

表 1　SD-Access 交换平台和部署建议

平台	支持的管理引擎	支持的面向交换矩阵的接口	推荐用作边缘节点	推荐用作边界节点	推荐用作控制平面节点
Catalyst 3850 和 3650 系列	—	板载端口和 10G/40G 网络模块端口	是	对于小规模部署（3850 光纤版本）	是
Catalyst 4500-E 系列	管理引擎 8-E	管理引擎上行链路端口	是	否	否
Catalyst 9300 系列	—	板载端口和 10G/40G/ 多千兆网络模块端口	是	否	否
Catalyst 9400 系列	管理引擎 1	管理引擎和线卡端口	是	否	否
Catalyst 6807 XL 交换机和 Catalyst 6500-E 系列	管理引擎 6T 和管理引擎 2T	管理引擎上行链路端口（仅管理引擎 6T） C6800 10G 系列 WS-X6900 系列	否	对于现有拓扑（需要 DHCP 服务器作用域分配策略）	是
Catalyst 6880-X 和 6840-X 系列	—	板载端口和端口卡端口	否	对于现有拓扑（需要 DHCP 服务器作用域分配策略）	是
Nexus 7700 系列	管理引擎 2E	M3 系列	否	对于大规模 40G/100G 部署（需要 DHCP 服务器作用域分配策略）	否（需要手动配置专用的外部控制平面节点）
Catalyst 9500 系列	—	板载端口	否	是	是

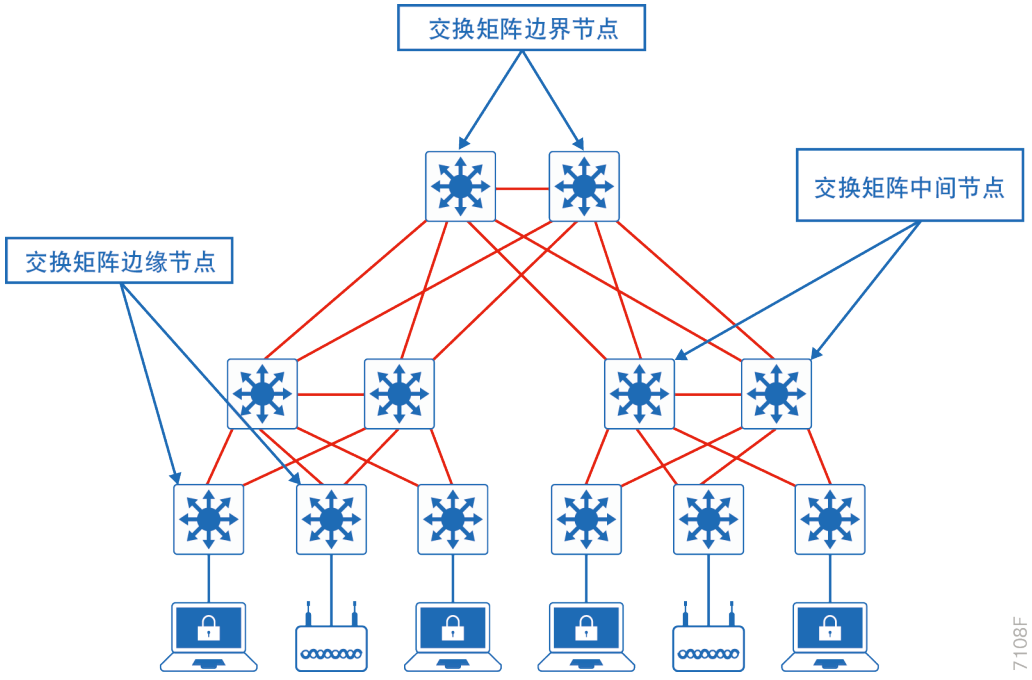
表 2　SD-Access 路由/无线平台和部署建议

平台	支持的管理引擎	支持的面向交换矩阵的接口	推荐用作边缘节点	推荐用作边界节点
云服务路由器 1000V 系列	-	-	-	是
思科 4000 系列集成多业务路由器（适用于 SD-Access 1.0 的 ISR 4450/4430）	板载局域网端口，以及路由局域网网络接口模块和增强服务模块端口	否	是	否
思科 ASR 1000-X 和 1000-hX 系列汇聚多业务路由器	板载局域网端口、以太网线卡和以太网共享端口适配器	否	是	是（大规模部署）
8540、5520 和 3504 系列无线控制器	通过关联的第二代和第一代 802.11AC 技术交换矩阵模式 AP 网络端口	否	否	无线客户端的控制平面代理

物理拓扑

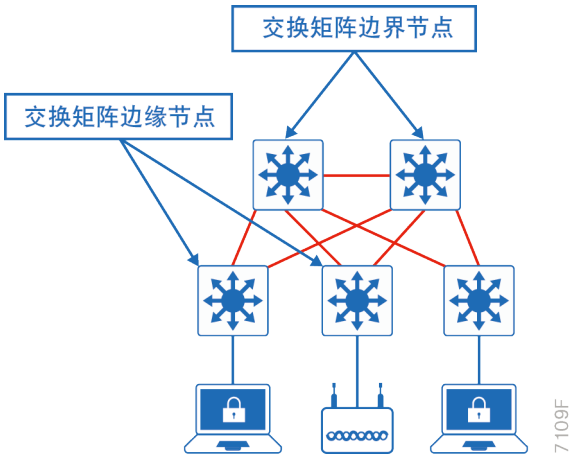
SD-Access 拓扑应该将网络划分为模块化的组，并遵守与分层设计相关的相同设计原则和最佳实践。您要采用模块化设计创建可在整个网络中复制的设计元素。下例显示了一个三层园区设计的物理拓扑，其中的所有节点均为双宿节点，以等价链路提供负载均衡、冗余和快速收敛等功能。虽然该拓扑中所绘的边界位于园区核心，但该边界也可与核心分开，在另一个汇聚点配置。每个汇聚层的交叉链路用于在上行链路出现故障时实现最佳路由。

图 7　三层 SD-Access 交换矩阵拓扑



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。

图 8　两层 SD-Access 交换矩阵拓扑



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退出点中心。不过，也可以使用其他物理拓扑。以交换矩阵作为传输网络的拓扑应该精心规划，确保实现最佳转发。如果实施边界节点的节点并非退出流量的汇聚点，则当流量在边界退出交换矩阵然后循原路折回实际汇聚点时，就会导致次优路由的结果。

底层网络设计

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 中心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：

- **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。
- **第 3 层接入设计** – 使用第 3 层路由网络作为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。
- **使用点对点链路** – 点对点链路可提供最快的收敛时间，因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典型。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。
- **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 可达性。在交换矩阵部署中，可以通过专用的 IGP 流程在 SD-Access 交换矩阵实施单区域 IGP 设计。用于交换矩阵内部链路的地址空间不需要在交换矩阵外部通告，并且可以在多个交换矩阵间重复使用。
- **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。作为一种最佳实践，请使用 /32 主机掩码。要传播环回主机路由，请使用路由标记，以便实现一种只重新分发环回地址的简便机制，避免维护前缀列表。

底层自动化

通过在 Cisco DNA 中心里使用思科网络即插即用服务，可以实现底层配置的完全自动化。在非绿场部署的情况下，您需要手动创建底层。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），但前面列出的底层设计原则仍然适用。

要自动部署底层，Cisco DNA 中心需要使用 IP 访问直接连接到新底层设备的种子设备。其余设备则使用逐跳 CDP 发现和调配进行访问。

技术提示

SD-Access 1.0 解决方案支持使用 Catalyst 3850/3650 和 Catalyst 9000 系列交换机实现底层自动化。有关其他平台，请参阅您的软件版本的相应版本说明以确认是否支持。

重叠交换矩阵设计

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可用于重叠内流量分段的可扩展组信息。部署虚拟网络时，应考虑以下设计注意事项：

- **根据网络要求的需要进行虚拟化** - 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。您可以从默认的局域网交换矩阵开始，也可以创建一组自己特有的虚拟网络 (VN)，支持传输 SGT 进行组分段。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 VN 间通信。
- **减少子网并简化 DHCP 管理** - 在重叠中，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。
- **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 VN 的共享服务和其他 VN 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。

交换矩阵控制平面设计

交换矩阵控制平面节点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 中心将自动配置控制平面的功能。为实现冗余，应该部署两个控制平面节点以确保交换矩阵的高可用性，将负载分布在两个节点间。应该选择支持控制平面的设备，以支持符合组织需要的 HTDB、CPU 和内存需求。

交换矩阵边界设计

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，可能必须调整边界设计。有关详细信息，请参阅本指南后面的“端到端虚拟化注意事项”部分。

基础设施服务

SD-Access 不需要对现有基础设施服务进行任何更改，只有一些默认边界配置的 DHCP 服务器除外。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，该网关并非唯一的，重叠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。

要确定特定的 DHCP 中继源，需要在交换矩阵边缘的中继代理上使用具有电路 ID 插入信息选项的 DHCP 选项 82。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。电路 ID 中嵌入的 DHCP 中继信息用作具有高级 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，交换矩阵的 DHCP 服务器作用域配置可以与标准的非交换矩阵创建保持一样。当您使用具有此功能的边界节点时，边界节点将检查从 DHCP 服务器返回的 DHCP 提议。收到 DHCP 提议的边界节点引用嵌入的电路 ID 并将 DHCP 提议定向到正确的中继目的。

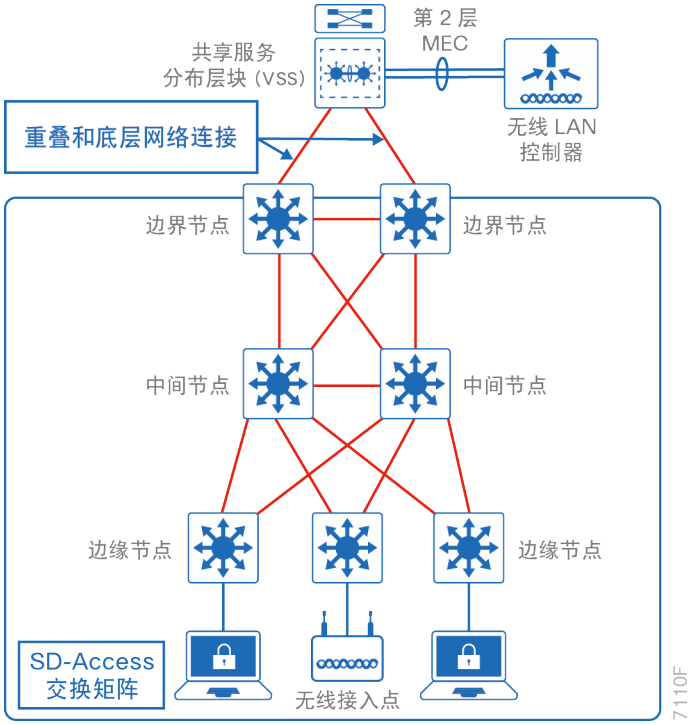
如果您使用的边界节点没有高级 DHCP 边界中继功能，则您需要修改 DHCP 服务器本身以便将 DHCP 提议定向到请求方的特定中继。必须配置 DHCP 服务器作用域选择条件，才能在创建提议时引用 DHCP 选项 82 电路 ID 信息，以包含特定的响应目的。有关实施 DHCP 服务器作用域、DHCP 选项和选择条件的信息，请参阅 SD-Access 部署指南。

交换矩阵无线集成

如前所述，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 控制平面仍然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，并且还能支持与 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。由于 WLC 需要同时连接到底层和交换矩阵重叠网络，因此必须通过任意基础设施将虚拟化 (VRF) 从边界节点扩展到 WLC 连接。本主题将在“虚拟化技术”部分详细介绍。

图 9　将无线组件集成到 SD-Access 中



非交换矩阵集中式无线选项

在无法将无缝漫游区域中的 WLC 和 AP 专门用于加入交换矩阵的情况下，可以选择传统的 CUWN 设计模型，它也称为*本地模式模型*。SD-Access 与 CUWN“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和 Cisco DNA 中心自动化的优势。

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 AP 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园区核心外的专用块。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 可位于交换矩阵内部或外部，无需对推荐的集中式无线局域网设计进行任何更改。

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摘要。

技术提示

在 SD-Access 1.0 解决方案中，SD-Access 交换矩阵内不支持融合接入和 FlexConnect。

安全/策略设计

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”方法。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法，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。
- **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** – 可以使用网络分段来控制对应用的访问；在交换环境中使用 IEEE 802.1AE 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 VN 内启用基于组的分段可以简化分层网络策略。使用 VN 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 VN 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。在大多数部署中，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。
- **在交换矩阵外部支持 TrustSec 的设备上** - 支持内联 TrustSec 的设备在第二层帧的 CMD 报头中传输 SGT 信息。这是推荐的 SD-Access 网络外部传输模式。
- **在交换矩阵外部通过不具备 TrustSec 功能的设备** - 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 www.cisco.com/go/trustsec。

设计规模注意事项

除表 1 中列出的平台角色建议外，为组织设计 SD-Access 时还应考虑以下规模参数。

技术提示

所列数字是 SD-Access 1.0 解决方案支持的最大限值。有关特定组件的其他限制，请查看相关硬件和软件的版本说明。

表 3 Cisco DNA 中心最大规模限制

SD-Access 结构	单个 Cisco DNA 中心的最大值	每个交换矩阵域的最大值
终端（有线/无线）- 跨所有交换矩阵域	20,000	20,000
每个交换矩阵边缘节点的终端	5,000	5,000
交换矩阵节点 - 跨所有交换矩阵域（路由器、交换机/交换机堆叠、WLC）	2,500	500
无线接入点 - 跨所有交换矩阵域（每个 AP 计为一个终端）	2,500	—
IP 池 - 跨所有交换矩阵域	500	500
站点	500	—
交换矩阵域	10	—
可扩展组标记 - 跨所有交换矩阵域	4000	1,000
策略 - 跨所有交换矩阵域	1,000	—
合同 - 跨所有交换矩阵域	500	—
控制平面节点	—	2
默认边界节点	—	2

表 4　SD-Access 边缘节点规模限制

	Catalyst 3850/3650	Catalyst 9300	Catalyst 4500 管理引擎 8-E	Catalyst 9400 管理引擎 1
虚拟网络	64	256	64	256
可扩展组标记	4000	8,000	2000	8,000
安全组 ACL	1500	5,000	64,000	18,000

表 5　SD-Access 边界节点规模限制

	Catalyst 3850（光纤）	Catalyst 9500	Catalyst 6800	Nexus 7700 管理引擎 2E	ASR 1000 和 ISR 4000
虚拟网络	64	256	512	500	4000
可扩展组标记	4000	32,000	30,000	64,000	64,000
安全组 ACL	1500	32,000	30,000	64,000	64,000
IP - SGT 的映射	2000	32,000	30,000	64,000	64,000
交换矩阵控制平面条目	4000	96,000	25,000	不支持	200,000
IPv4 路由数	8,000	48,000	48,000	1,000,000 (XL) 256,000（非 XL）	4,000,000 (16GB) 1,000,000 (8GB)
IPv4 主机条目	16,000	96,000	48,000	1,000,000 (XL) 256,000（非 XL）	4,000,000 (16GB) 1,000,000 (8GB)

端到端设计注意事项

在虚拟网络中，数据和控制平面在共享的网络基础设施上完全隔离。在 SD-Access 的情况下，位于一个 VN 中的用户完全隔离，不能与位于不同 VN 中的用户进行通信。交换矩阵边界节点负责将网络虚拟化扩展到 SD-Access 交换矩阵外。组织可能存在需要此类隔离的业务要求。网络虚拟化在某些垂直行业特定使用案例中可能非常实用，其中部分示例包括：

- **教育业** – 大学校园分为行政网络和学生宿舍网络。
- **零售业** – 隔离支持支付卡行业合规性的销售终端机。
- **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、患者访客接入和 HIPAA 合规性。
- **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。分离楼宇控制系统和视频监控设备。

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保持共享这些服务的不同虚拟网络之间相互隔离。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的安全防护层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** – 使用通用的无线局域网（单 SSID）提高射频性能和成本效率。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，只要它们支持虚拟网络。高级 DHCP 作用域选择条件、多个域和支持重叠地址空间等特殊功能是将服务扩展到单个网络外所需的某些功能。
- **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 通信** – 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 VN。

网络虚拟化技术

使用多 VRF 配置可以将 SD-Access 交换矩阵虚拟化扩展到交换矩阵边界之外。SD-Access VN 可以 1:1 或 N:1 映射到 SD-Access 交换矩阵外部的 VRF。有关端到端网络虚拟化的指南不属于本指南的范围。不过，此部分简要介绍了一些最常用的技术，您在进行网络虚拟化时可对这些技术加以研究。

设备级虚拟化

在同一台物理设备中，可以使用第 2 层和 3 层逻辑分离功能来扩展虚拟网络：

虚拟局域网

设备级虚拟化最基本的形式是使用不同的虚拟局域网（VLAN）隔离网络流量。这种形式的虚拟化应用于第 2 层设备，而且可以跨交换域扩展。VLAN 还可用于虚拟化路由器与需要通过同一物理接口连接到多个虚拟网络安全设备之间的点对点链路。

虚拟路由和转发

VRF 是用于在同一设备上创建多个第 3 层路由表的设备级虚拟化技术。VRF 可与现有第 2 层域绑定，为多个 VLAN 提供第 3 层边缘功能，也可在第 3 层路由接口之间绑定，以便扩展同一组接口上的多个虚拟化控制平面。

路径隔离

要对用于互联设备的路径保持路径隔离，有许多技术选择可以在设备间提供网络虚拟化。对于 SD-Access，建议使用的路径隔离技术是 VRF-Lite 和 MPLS VPN。具体设计通常取决于所需的虚拟网络数量。如果您预计所需 VRF 不止几个，则部署 MPLS VPN 可简化配置和管理。

VRF-Lite 端到端

在园区网络中，VRF-Lite 是逐跳部署的，在设备间使用 802.1Q 中继为每个虚拟网络隔离数据和控制平面。为便于操作，应该在每一跳上使用同一组 VLAN，并通过每 VN 地址系列使用 BGP，提供可用于简化共享服务路由泄漏的属性。

MPLS

虽然 MPLS 通常被视为运营商使用的技术，但在需要大量虚拟网络的大型企业中也比较常用；它主要见于广域网中，但也可扩展到园区网络。VRF-Lite 为大多数路由平台所通用，而 MPLS 则并非受到所有平台的支持。在边缘节点配合使用 VRF-Lite 和 MPLS VPN 是另一种可以考虑的设计选择。

技术提示

SD-Access 1.0 解决方案支持在交换矩阵边界节点切换 VRF-Lite。有关其他选项，请参阅您的软件版本的相应版本说明以确认是否支持。

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 中心从头开始自动调配网络架构，就可以轻而易举地创建 SD-Access 绿场网络。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 VN，将这些 VN 与通用服务（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 VN 进行分段和虚拟化，存在哪些将其扩展到交换矩阵外的要求？是否具备必要的基础设施，可以支持 TrustSec、VRF-Lite、MPLS、融合路由器或者扩展和支持分段和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绿场网络的变化形式。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。

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 - 术语表

AAA 身份验证、授权和记帐

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

CMD 思科元数据

Cisco DNA 思科全数字化网络架构

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 软件定义的接入

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

VTEP 虚拟可扩展局域网隧道终端

VXLAN 虚拟可扩展局域网

您可以使用反馈表提供有关本指南的评论和建议。

美洲总部
思科系统公司
San Jose, CA

亚太总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
思科 Systems International BV 阿姆斯特丹
荷兰

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。