CISCO VALIDATED DESIGN

Software-Defined Access Design Guide

August 2017

Table of Contents

Cisco Digital Network Architecture and Software-Defined Access Introduction

Cisco® Digital Network Architecture (DNA) provides a roadmap to digitization and a path to realize immediate benefits of network automation, assurance, and security. Cisco's Software-Defined Access (SD-Access) architecture is the Cisco DNA evolution from traditional campus LAN designs. SD-Access uses DNA Center for designing, provisioning, applying policy, and providing campus wired and wireless network assurance for an intelligent network. Campus fabric technology, an integral part of SD-Access, introduces programmable overlays enabling easy-to-deploy network virtualization across the wired and wireless campus. In addition to network virtualization, campus fabric technology provides software-defined segmentation and policy enforcement based on user identity and group membership. Software-defined segmentation is seamlessly integrated using Cisco TrustSec technology, providing micro-segmentation through the use of scalable groups within a virtual network. Using DNA Center to automate the creation of virtual networks provides reduction in operational expenses, coupled with the advantage of reduced risk with integrated security and improved network performance provided by the assurance and analytics capabilities.

This guide provides an overview of the requirements driving the evolution of campus network designs, followed by a discussion about the latest technologies and designs that are available for building an SD-Access network to address those requirements. This guide is a companion to the associated deployment guides for SD-Access, which provide configurations required to implement the designs as described in this guide. The intended audience is a technical decision maker who wants to understand Cisco's campus offerings and to learn about the technology options available and the leading practices for designing the best network for the needs of an organization.

For related design guides, deployment guides, and white papers, see the following page:

http://www.cisco.com/go/designzone

NETWORK REQUIREMENTS FOR THE DIGITAL ORGANIZATION

With digitization, software applications are evolving from simply supporting business processes to becoming, in some cases, the primary source of business revenue and competitive differentiation. Organizations are now constantly challenged by the need to scale their network capacity in order to quickly react to, and support the growth of, application demands. Because the campus LAN is the network through which users and devices within a location access applications, campus wired and wireless LAN capabilities should be enhanced to support those changing needs.

The following are key requirements that are driving the evolution of existing campus networks.

Flexible Ethernet Foundation for Growth and Scale

- **Increased capacity of wireless access points**—The bandwidth demands on wireless access points (APs) with the latest 802.11ac Wave 2 technology now exceed 1 Gbps, and the IEEE has now ratified the 802.3bz standard that defines 2.5 Gbps and 5 Gbps Ethernet. Cisco Catalyst Multigigabit technology supports that bandwidth demand without requiring an upgrade of the existing copper Ethernet wiring plant.
- **Additional power requirements from Ethernet devices**—New devices may require higher power to operate, such as lighting, surveillance cameras, virtual desktop terminals, remote access switches, and APs. Your access layer design should have the ability to support power over Ethernet with 60W per port, offered with Cisco Universal Power Over Ethernet, and the access layer should also provide PoE perpetual power during switch upgrade and reboot events. The Cisco Catalyst 9000 Series access layer switches are perpetual PoE-capable and ready for 100W per port, as that technology becomes available.
- **Increased bandwidth needs**—Bandwidth needs are doubling potentially multiple times over the lifetime of a network, resulting in new networks needing to be prepared to aggregate using 10 Gbps Ethernet to 40 Gbps to 100 Gbps capacities over time.
- **Simplified Deployment and Automation**—Network device configuration and management through a centralized controller using open APIs allow for very fast, lower-risk deployment of network devices and services through UI and existing orchestration systems.

Network Integrated Security

- **Consistent Wired and Wireless Security Capabilities**—Security capabilities described below should be consistent whether a user is connecting to a wired Ethernet port or connecting over the wireless LAN.
- **Network Assurance and Analytics**—Proactively predict network- and security-related risks by using telemetry to improve the performance of the network, devices, and applications, even with encrypted traffic.
- **Identity services**—Identifying users and devices connecting to the network provides the contextual information required to implement security policies for access control, network segmentation by using scalable group membership and mapping of devices into virtual networks (VNs).
- **Group-based policies**—Creating security policies based on user group information provides a much easier and scalable way to deploy and manage security policies. Traditional access control lists (ACLs) can be difficult to implement, manage, and scale because they rely on network constructs such as IP addresses and subnets.
- **Software-defined segmentation**—Scalable group tags (SGTs), also known as *security group tags*, assigned from group-based policies can be used to segment a network in order to achieve data plane isolation within physical and virtual networks.
- **Network virtualization**—The capability to share a common infrastructure while supporting multiple VNs with isolated data and control planes enables multi-tenancy and security.

Software-Defined Access Architecture

The SD-Access architecture is supported by campus fabric technology, which enables the use of virtual networks (overlay networks) running on a physical network (underlay network) in order to create alternative topologies to connect devices. Overlay networks are commonly used to provide Layer 2 and Layer 3 logical networks with virtual machine mobility in data center fabrics (examples: ACI, VXLAN, and FabricPath). Overlay networks are also used in wide-area networks to provide secure tunneling from remote sites (examples: MPLS, DMVPN, and GRE). This section provides information about the SD-Access architecture elements. SD-Access design recommendations are covered in the Design Considerations section.

UNDERLAY NETWORK

The underlay network is defined by the physical switches and routers that are part of the SD-Access network. All network elements of the underlay must establish IP connectivity via the use of a routing protocol. Theoretically, any topology and routing protocol can be used, but the implementation of a well-designed Layer 3 foundation to the campus edge is highly recommended to ensure performance, scalability, and high availability of the network. In the SD-Access architecture, end-user subnets are not part of the underlay network.

Tech Tip

DNA Center can automate the deployment of the underlay network using Cisco Network Plug and Play.

Tech Tip

The SD-Access 1.0 solution supports IPv4 underlay networks. For IPv6 underlay networks, see the release notes for your software version in order to verify support.

OVERLAY NETWORK

An overlay network runs over the underlay in order to create a virtualized network. The data plane traffic and control plane behavior is contained within each virtualized network, maintaining isolation among the networks in addition to isolation from the underlay network. Virtualization is implemented within the SD-Access fabric by encapsulating user traffic over IP tunnels that are sourced and terminated at the boundaries of the fabric. Network virtualization extending outside of the fabric is preserved using traditional virtualization technologies such as VRF-Lite and MPLS VPN. Overlay networks can run across all or a subset of the underlay network devices. Multiple overlay networks can run across the same underlay network to support multi-tenancy through virtualization.

IPv4 multicast forwarding is delivered in the overlay at the fabric border and fabric edge nodes, using LISP head-end replication. You integrate PIM routing from the border with the adjacent multicast router outside of the fabric. DNA Center configures PIM, IGMP, and LISP multicast support.

Tech Tip

The SD-Access 1.0 solution supports both PIM SM and PIM SSM.

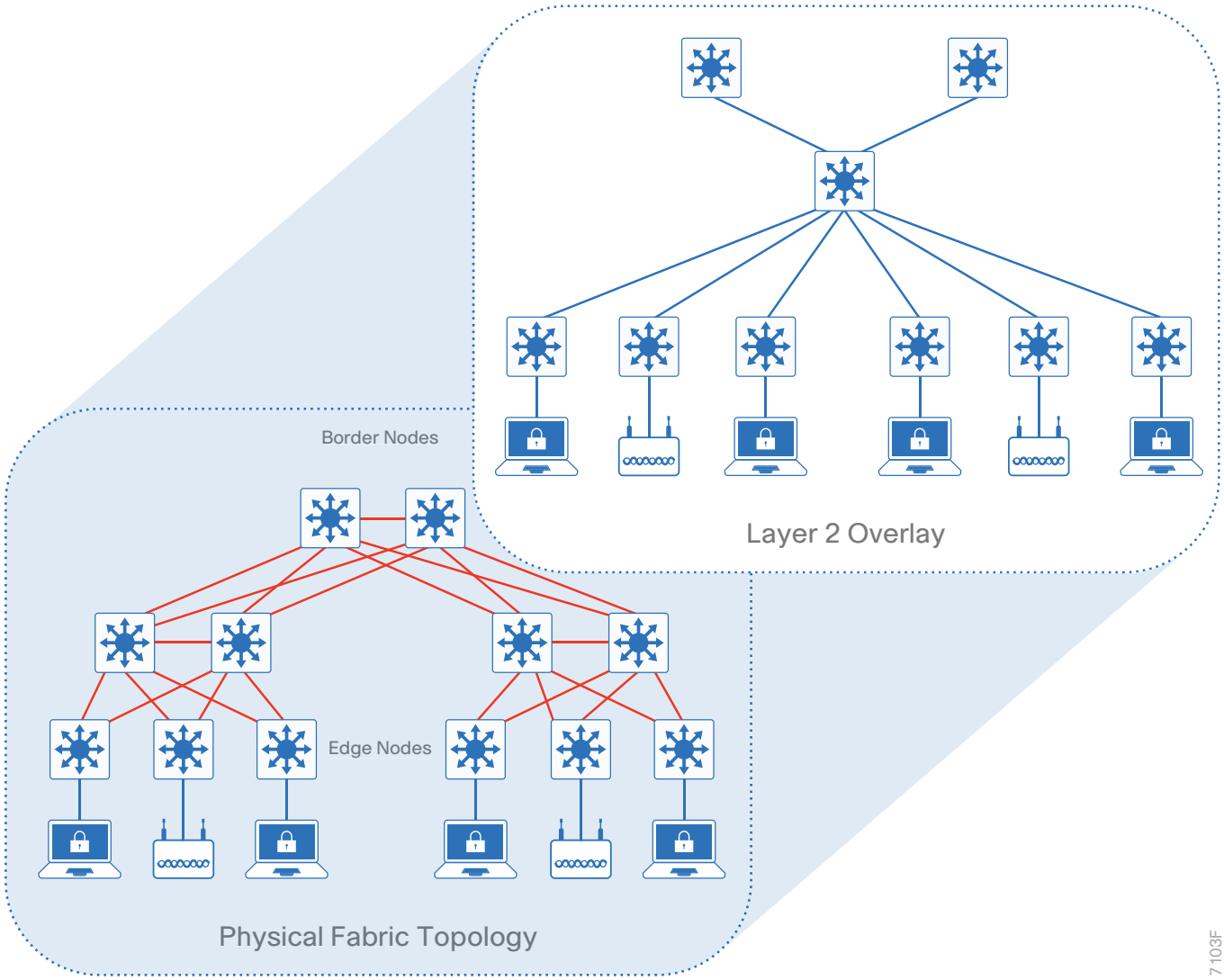
Layer 2 Overlays

Layer 2 overlays emulate a LAN segment to transport IP and non-IP frames. Layer 2 overlays carry a single subnet over the Layer 3 underlay. Layer 2 overlays are useful in emulating physical topologies and are subject to Layer 2 flooding.

Tech Tip

The SD-Access 1.0 solution supports transport of only IP frames in Layer 2 overlays, without Layer 2 flooding. For transport of non-IP frames and Layer 2 flooding, see the release notes for your software version in order to verify support.

Figure 1 *Layer 2 overlay—connectivity logically switched*



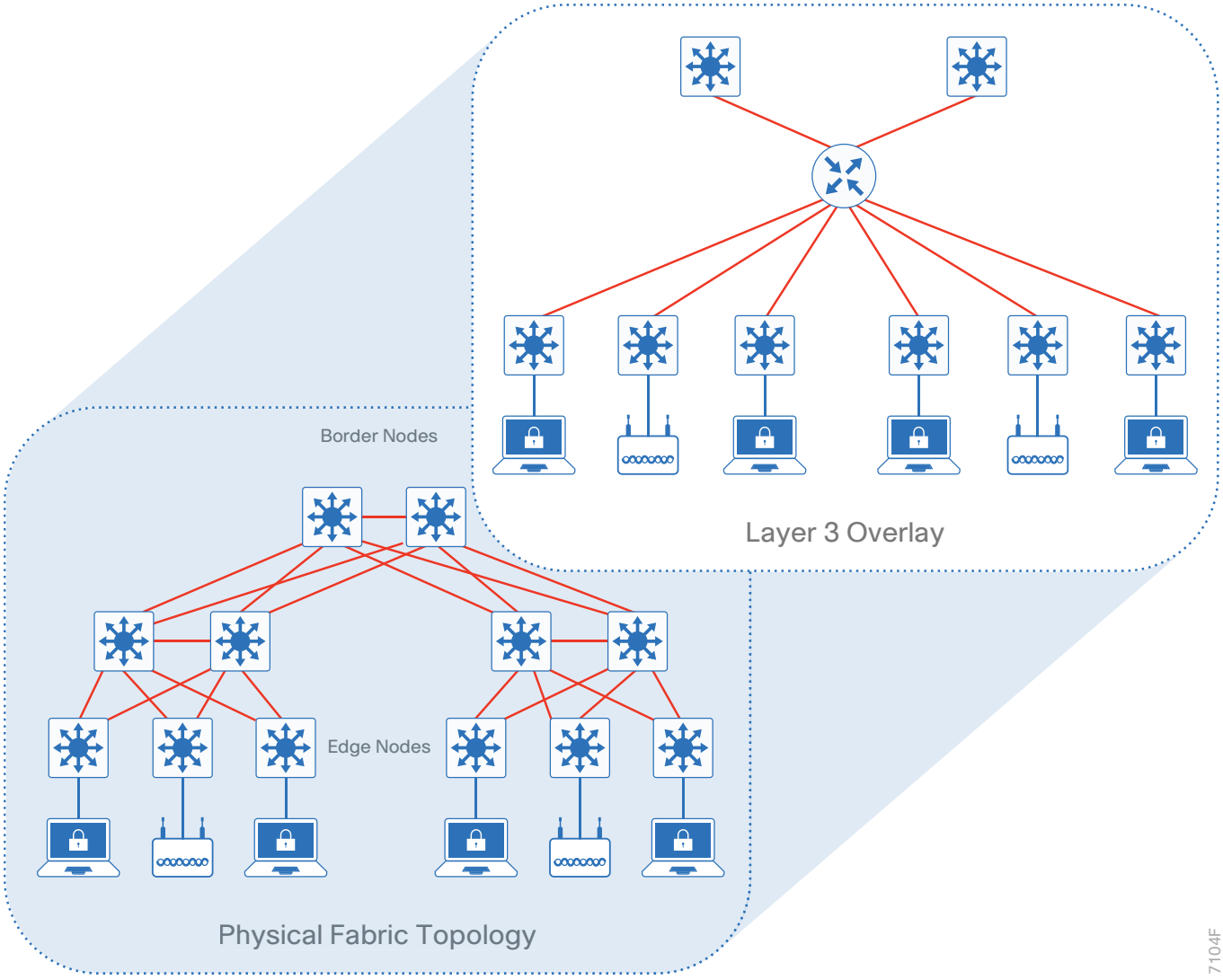
Layer 3 Overlays

Layer 3 overlays abstract IP based connectivity from physical connectivity and allow multiple IP networks as part of each virtual network. Overlapping IP address space is supported across different Layer 3 overlays as long as the network virtualization is preserved outside of the fabric, using existing network virtualization functions such as VRF-Lite and MPLS L3VPN.

Tech Tip

The SD-Access 1.0 solution supports IP4 overlays. Overlapping IPs is not supported for wireless clients on the same WLC. For IPv6 overlays, see the release notes for your software version in order to verify support.

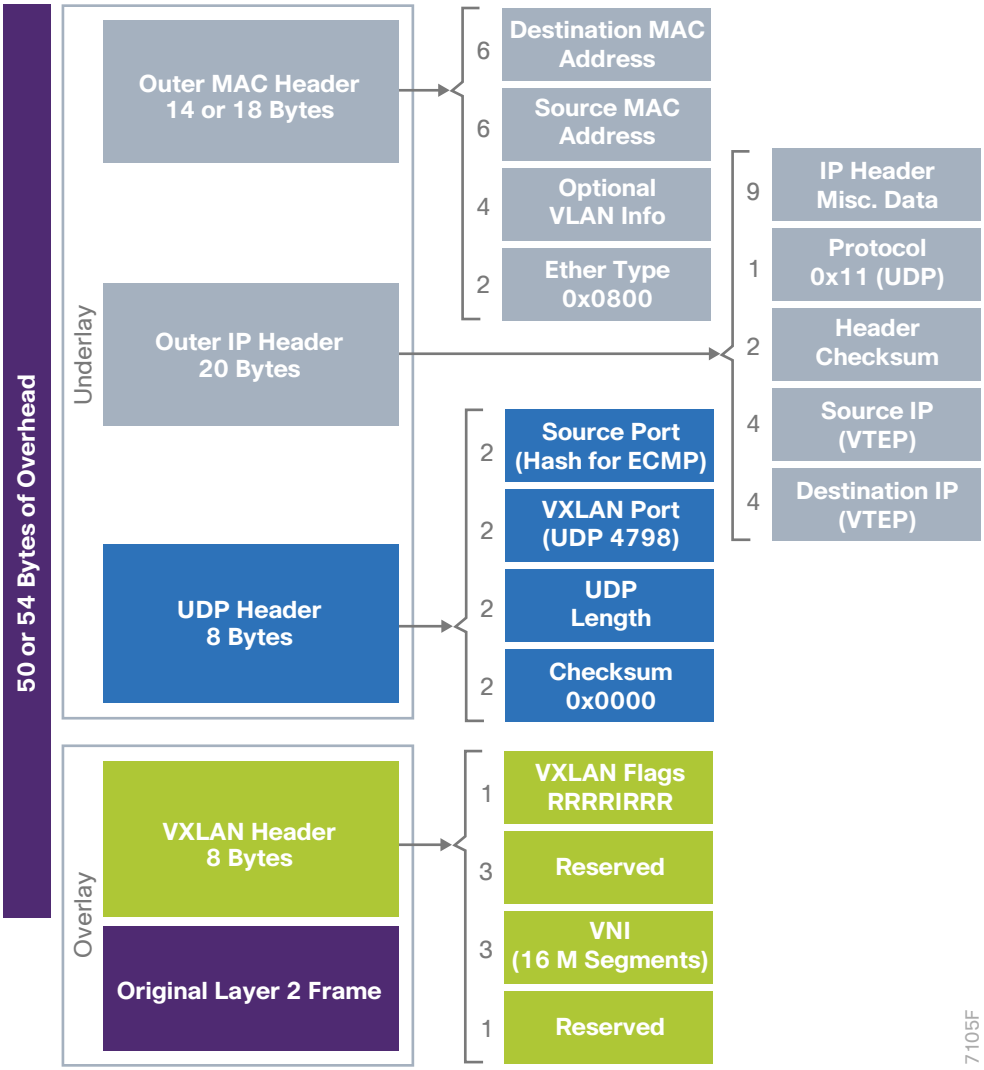
Figure 2 *Layer 3 overlay–connectivity logically routed*



FABRIC DATA PLANE

RFC 7348 defines the use of virtual extensible LAN (VXLAN) as a way to overlay a Layer 2 network on top of a Layer 3 network. Using VXLAN, you tunnel the original Layer 2 frame using UDP/IP over the Layer 3 network. The tunnel interface at each node is called a *VXLAN tunnel endpoint* (VTEP). VTEPs rely on data-plane learning or a control plane in order to determine the remote endpoint to VTEP mapping for traffic encapsulation. Each overlay network is called a *VXLAN segment* and is identified using a 24-bit VXLAN network identifier (VNI), which supports up to 16 million VXLAN segments.

Figure 3 *RFC 7348 VXLAN header*



The SD-Access fabric uses the VXLAN data plane in order to provide transport of the full original Layer 2 frame and additionally uses Locator/ID Separation Protocol (LISP) as the control-plane in order to resolve endpoint-to-VTEP mappings. The SD-Access fabric replaces 16 of the reserved bits in the VXLAN header in order to transport up to 64,000 SGTs.

The VNI maps to a virtual routing and forwarding (VRF) instance for Layer-3 overlays, whereas a Layer-2 VNI maps to a VLAN broadcast domain, both providing the mechanism to isolate data and control plane to each individual virtual network. The SGT carries group membership information of users and provides data-plane segmentation inside the virtualized network.

FABRIC CONTROL PLANE

RFC 6830 and other RFCs define LISP as a network architecture and set of protocols that implement a new semantic for IP addressing and forwarding. In traditional IP networks, the IP address is used to identify both an endpoint and its physical location as part of a subnet assignment on a router. In a LISP-enabled network, an IP address is used as the endpoint identifier (EID) for a device, and an additional IP address is used as a routing locator (RLOC) to represent the physical location of that device (typically a loopback address of the router to which the EID is attached). The EID and RLOC combination provides the necessary information for traffic forwarding. The RLOC address is part of the routing domain, and the EID can be assigned independently of the location.

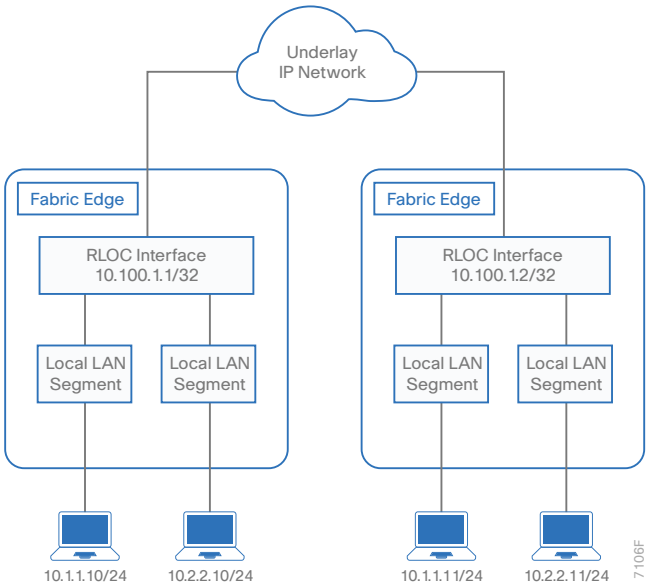
The LISP architecture requires a mapping system that stores and resolves EIDs to RLOCs. This is analogous to using DNS to resolve IP addresses for host names and is also similar to the previously mentioned VTEP mapping in the VXLAN data plane. EID prefixes (either IPv4 addresses with /32 "host" masks or MAC addresses) are registered into the map server along with their associated RLOCs. When sending traffic to an EID, a source RLOC queries the mapping system in order to identify the destination RLOC for traffic encapsulation.

Although a full understanding of LISP and VXLAN is not required to deploy a fabric in SD-Access, it is helpful to understand how these technologies support the deployment goals. Included benefits provided by the LISP architecture are:

- **Network virtualization**—A LISP Instance ID is used to maintain independent VRF topologies. From a data-plane perspective, the LISP Instance ID maps to the VNI.
- **Subnet stretching**—A single subnet can be extended to exist at multiple RLOCs. The separation of EID from RLOC enables the capability to extend subnets across different RLOCs. The RLOC in the LISP architecture represents the VTEP functionality in VXLAN as it is the ingress and egress tunnel used to encapsulate EID traffic over a Layer 3 network. As a result of the availability of the anycast gateway across multiple RLOCs, the EID client configuration (IP address, subnet, and gateway) can remain unchanged, even as the client moves across the stretched subnet to different physical attachment points.
- **Smaller routing tables**—Only RLOCs need to be reachable in the global routing table. Local EIDs are cached at the local node while remote EIDs are learned through conversational learning. *Conversational learning* is the process of populating forwarding tables with only endpoints that are communicating through the node. This allows for efficient use of forwarding tables.

The following diagram shows an example of two subnets that are part of the overlay network and are stretched across routers that are physically separated. The RLOC interface is the only routable address that is required to establish connectivity between endpoints of the same or different subnet.

Figure 4 *LISP sample topology*



WIRELESS INTEGRATION

SD-Access supports traditional Cisco Unified Wireless Network (CUWN) local-mode configurations "over the top" as a non-native service. In this mode, the SD-Access fabric is simply a transport network for the wireless traffic. Alternatively, you gain advantages by integrating wireless natively into SD-Access using two additional components—fabric wireless controllers and fabric mode APs. The fabric controllers are supported Cisco Wireless LAN Controllers (WLCs) configured to communicate with the fabric LISP control plane, registering L2 client MAC addresses, SGT, and L2 VNI information. The fabric mode APs are existing Cisco 802.11AC Wave 2 and Wave 1 APs associated with the fabric wireless controller and configured with fabric-enabled SSIDs. The APs are responsible for communication with wireless endpoints, and in the wired domain, the APs assist the VXLAN data plane by encapsulating and de-encapsulating traffic at the connected edge node.

Tech Tip

For differences between Wave 2 and Wave 1 AP feature support, see the release notes for your software version.

Tech Tip

DNA Center for the SD-Access 1.0 solution supports automation for fabric wireless. To verify support for non-fabric modes of operation, see the release notes for your software version.

Fabric wireless controllers manage and control the fabric mode APs using the same model as the traditional centralized model of local-mode controllers, offering the same operational advantages, such as mobility control and radio resource management. A significant difference is that traffic carried from wireless endpoints on fabric SSIDs avoids CAPWAP encapsulation and forwarding from the APs to the central controller. Instead, communication from wireless clients is VXLAN-encapsulated by fabric-attached APs. This difference enables a distributed data plane with integrated SGT capabilities. Traffic is forwarded directly to the VTEP, taking the optimum path through the SD-Access fabric to the destination with consistent policy, regardless of wired or wireless endpoint connectivity. Support for wireless guest is enabled by placing a guest fabric border node on a DMZ segment using a dedicated VN for guest users, isolating them. DNA Center automates and manages the workflow for implementing the full guest solution.

The SD-Access wireless control plane for the APs uses a CAPWAP tunnel to the WLC, similar to the traditional CUWN control plane. However, the WLC integration with the SD-Access LISP control plane supports wireless clients roaming to APs across the fabric. The LISP control plane inherently supports the roaming feature by updating its host-tracking database with any changes for a wireless client EID associated with a new RLOC.

Although the fabric mode APs are used for VXLAN traffic encapsulation for wireless traffic while it moves between the wireless and the wired portions of the fabric, the APs are not edge nodes. Instead, APs connect directly to edge node switches using VXLAN tunnels and rely on those switches to provide fabric services, such as the Layer 3 anycast gateway.

Integrating the wireless LAN into the fabric enables the fabric advantages for the wireless clients, including addressing simplification, mobility with stretched subnets, and end-to-end segmentation with policy consistency. Wireless integration also enables the WLC to shed data plane forwarding duties while continuing as the centralized services and control plane for the wireless domain.

SOLUTION MANAGEMENT

As previously mentioned, a full understanding of LISP and VXLAN is not required to deploy the fabric in SD-Access. Nor is there a requirement to know the details of how to configure each individual network component and feature to create the consistent end-to-end behavior offered by SD-Access. Instead, you use Cisco DNA Center—an intuitive centralized management system to design, provision, and apply policy across the wired and wireless SD-Access network.

In addition to automation for SD-Access, DNA Center offers traditional applications to improve an organization's efficiency, such as software image management, along with new capabilities, such as device health dashboards and 360° views, as listed in the Solutions Components section.

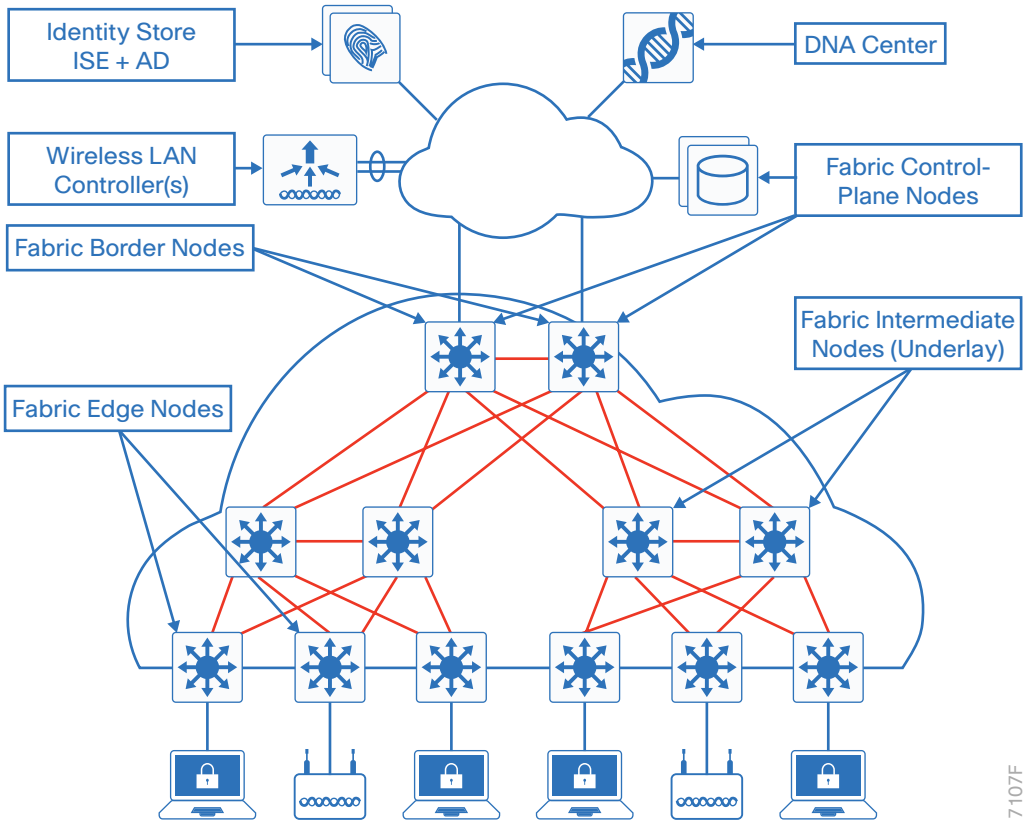
In summary, DNA Center is integral to SD-Access, enabling automation of device deployments into the network providing the speed and consistency required for operational efficiency. Organizations then benefit from lower cost and reduced risk when deploying and maintaining their networks.

Policy management with identity services integrates into the SD-Access network using an external repository hosted by the Cisco Identity Services Engine (ISE). ISE couples with the SD-Access controller for dynamic mapping of users and devices to scalable groups, simplifying end-to-end security policy management and enforcement at a greater scale than traditional network policy implementations relying on IP access-lists.

Solution Components

The SD-Access solution combines the DNA Center enterprise controller, identity services, and wired and wireless fabric functionality. Within the SD-Access solution, the fabric is composed of fabric control plane nodes, edge nodes, intermediate nodes, and border nodes. Wireless integration adds fabric WLC and fabric mode AP components. This section describes the functionality for each role, how the roles map to the physical campus topology, and the components required for solution management, wireless integration, and policy application.

Figure 5 *SD-Access solution and fabric components*



CONTROL PLANE NODE

The SD-Access fabric control plane node is based on the LISP Map-Server (MS) and Map-Resolver (MR) functionality combined on the same node. The control plane node functionality is instantiated on the border node or a dedicated node. The control plane node enables the following functions:

- **Host Tracking Database**—The host tracking database (HTDB) is a central repository of EID-to-fabric-edge node bindings.
- **Map-Server**—The LISP MS is used to populate the HTDB from registration messages from fabric edge devices.
- **Map-Resolver**—The LISP MR is used to respond to map queries from fabric edge devices requesting RLOC mapping information for destination EIDs.

EDGE NODE

The SD-Access fabric edge nodes are the equivalent of an access layer switch in a traditional campus design. The edge nodes implement a Layer 3 access design with the addition of the following fabric functions:

- **Endpoint registration**—After an endpoint is detected by the fabric edge, it is added to a local host tracking database called the EID-table. The edge device also issues a LISP map-register message in order to inform the control plane node of the endpoint detected so that it can populate the HTDB.
- **Mapping of user to virtual network**—Endpoints are placed into virtual networks by assigning the endpoint to a VLAN associated with a LISP instance. The mapping of endpoints into VLANs can be done statically or dynamically using 802.1X. Optionally, an SGT is assigned to provide segmentation and policy enforcement at the fabric edge.
- **Anycast Layer 3 gateway**—A common gateway (IP and MAC addresses) can be used at every node that shares a common EID subnet in order to provide for optimal forwarding and mobility across different RLOCs.
- **LISP forwarding**—Instead of a typical routing-based decision, the fabric edge nodes query the map server in order to determine the RLOC associated with the destination IP and use that information to encapsulate the traffic in VXLAN. In case of a failure to resolve the destination RLOC, the traffic is sent to the default fabric border in which the global routing table is used for forwarding. The response received from the map server is stored in the LISP map-cache, which is merged to the CEF table and installed in hardware. If VXLAN-encapsulated traffic is received at the fabric edge for an endpoint not locally connected, a LISP solicit map request is sent to the sending fabric edge in order to trigger a new map request; this addresses the case where the endpoint may be present on a different fabric edge switch.

INTERMEDIATE NODE

The fabric intermediate nodes are part of the Layer 3 network that interconnects the edge nodes to border nodes. In case of a three-tier campus design using a core, distribution, and access, the intermediate nodes are the equivalent of distribution switches. Intermediate nodes only route IP traffic inside the fabric. No VXLAN encapsulation/de-encapsulation or LISP control plane messages are required from the intermediate node, which only has the additional requirement to accommodate the additional size of IP packets containing the embedded VXLAN information.

BORDER NODE

The fabric border nodes serve as the gateway between the SD-Access fabric domain and the network outside of the fabric. The fabric border node is responsible for network virtualization inter-working and SGT propagation from the fabric to the rest of the network. The fabric border nodes can be configured as the gateway for specific network addresses such as WAN networks or in a default border role useful for the Internet or a common exit point from a fabric. Border nodes implement the following functions:

- **Advertisement of EID subnets**—The fabric border runs either an interior gateway protocol (IGP) or border gateway protocol (BGP) as a routing protocol in order to advertise the EID prefixes outside of the fabric and traffic destined to EID subnets from outside the fabric goes through the border nodes. These EID prefixes appear only on the routing tables at the border—throughout the rest of the fabric, the EID information is accessed using the fabric control plane node.
- **Fabric domain exit point**—The default fabric border is the gateway of last resort for the fabric edge nodes. This is implemented using LISP Proxy Tunnel Router functionality. Also possible are non-default fabric borders connected to networks with a well-defined set of IP subnets, adding the requirement to advertise those subnets into the fabric.

- **Mapping of LISP instance to VRF**—The fabric border can extend network virtualization from inside the fabric to outside the fabric by using external VRF instances in order to preserve the virtualization.
- **Policy mapping**—The fabric border node also maps SGT information from within the fabric to be appropriately maintained when exiting that fabric. Tags from the VXLAN header are mapped to Cisco Meta Data (CMD) when inline tagging capabilities are used, or alternatively the tags are transported by SGT exchange protocol (SXP), allowing for seamless integration with the Cisco TrustSec solution.

FABRIC WIRELESS LAN CONTROLLER

The fabric WLC integrates the control plane for wireless into the fabric control plane. Both fabric WLCs and non-fabric WLCs provide AP image and configuration management, client session management, and mobility services. Fabric WLCs provide additional services for fabric integration by registering MAC addresses of wireless clients into the host tracking database during wireless client join events and by supplying fabric edge RLOC location updates during client roam events.

A key difference with non-fabric WLC behavior is that fabric WLCs are not active participants in the data plane traffic-forwarding role for the SSIDs that are fabric enabled—fabric mode APs directly forward traffic through the fabric for those SSIDs.

FABRIC MODE APS

The fabric mode APs are Cisco 802.11AC Wave 2 and Wave 1 APs associated with the fabric WLC that have been configured with one or more fabric-enabled SSIDs. Fabric mode APs continue to support the same 802.11AC wireless media services that traditional APs support; apply AVC, QoS, and other wireless policies; and establish the CAPWAP control plane to the fabric WLC. Fabric APs join as local-mode APs and must be directly connected to the fabric edge node switch to enable fabric registration events, including RLOC assignment via the fabric WLC.

When wireless clients connect to a fabric mode AP and authenticate into the fabric-enabled wireless LAN, the WLC updates the fabric mode AP with the client L2 VNID and an SGT supplied by ISE, and then proxy-registers the wireless client L2 EID into the LISP control plane on behalf of the fabric edge node switch. After the initial connectivity is established, wireless client communication is VXLAN-encapsulated at the AP using the L2 VNI information to the directly-connected fabric edge switch. The fabric edge switch maps the client traffic into the appropriate VLAN interface associated with the VNI for forwarding across the fabric and registers the wireless client IP addresses with the control plane database.

IDENTITY SERVICES ENGINE

Cisco ISE is an integral part of SD-Access for policy implementation, enabling dynamic mapping of users and devices to scalable groups and simplifying end-to-end security policy enforcement. ISE integrates with the SD-Access controller by using Cisco Platform Exchange Grid (pxGrid) and RESTful APIs for exchange of client information and automation of fabric-related configurations on ISE.

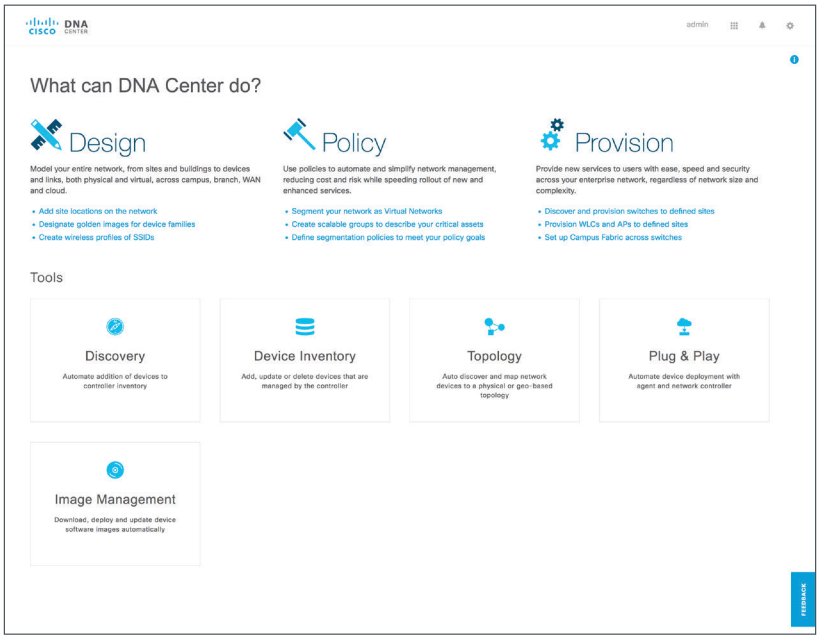
The SD-Access solution integrates Cisco TrustSec by supporting group-based policy end-to-end, including SGT information in the VXLAN headers for data plane traffic, while supporting multiple VNs using unique VNI assignments. Groups, policy, authentication, authorization, and accounting (AAA) services, and endpoint profiling are driven by ISE and orchestrated by DNA Center's policy authoring workflows.

Scalable groups are identified by the SGT, a 16-bit value that is transmitted in the VXLAN header. SGTs are centrally created, managed, and administered by Cisco ISE. ISE and DNA Center are tightly integrated through RESTful APIs, with management of the policies driven by DNA Center.

CISCO DNA CENTER

At the heart of automation of the SD-Access solution is Cisco DNA Center. DNA Center is an application that runs on Application Policy Infrastructure Controller-Enterprise Module (APIC-EM), using services provided by the controller for planning and preparation, installation and integration.

Figure 6 *DNA Center Dashboard*



DNA Center centrally manages four major workflow areas.

- **Design**—Configures device global settings, network site profiles for physical device inventory, DNS, DHCP, IP addressing, software image management, plug-and-play, and user access.
- **Policy**—Defines business intent for provisioning into the network, including creation of virtual networks, assignment of endpoints to virtual networks, and policy contract definition for groups.
- **Provision**—Provisions devices for management and creates fabric domains, control plane nodes, border nodes, edge nodes, fabric wireless, CUWN wireless, and external connectivity.
- **Assurance**—Enables health scores dashboard, client/device 360° views, node, client, and path traces.

DNA Center supports integration via open APIs. For example, Infoblox IP address management and policy enforcement integration with ISE are available through DNA Center. A comprehensive set of northbound RESTful APIs enables automation, integration, and innovation.

- All controller functionality is exposed through northbound RESTful APIs.
- Organizations and ecosystem partners can easily build new applications.
- All northbound RESTful API requests are governed by the controller RBAC mechanism.

DNA Center is key to enabling automation of device deployments into the network providing the speed and consistency required for operational efficiency. Organizations using DNA Center then are able to benefit from lower cost and reduced risk when deploying and maintaining their networks.

SD-Access Design Considerations

Designing for an SD-Access fabric is not a one-design-fits-all proposition. The scale of a fabric can be as small as an access-distribution block or as big as a three-tier campus deployment. In a single network, multiple fabrics can be deployed as long as the fabric elements are assigned to a single fabric only.

PLATFORM ROLES AND RECOMMENDATIONS

Choose your SD-Access network platform based on capacity and capabilities required by the network, considering the recommended functional roles.

Tech Tip

To achieve the functionality shown, you must meet minimum software release requirements. Some of the platforms are not listed as recommended for a particular role, even though the platform includes the functionality. For more information, see the software release notes for your platform and refer to CVD deployment guides for as-tested code versions.

Table 1 SD-Access switching platforms and deployment recommendations

Platform	Supported Supervisor	Supported Fabric-facing Interfaces	Recommended as Edge Node	Recommended as Border Node	Recommended as Control Plane Node
Catalyst 3850 and 3650 Series	–	Onboard Ports and 10G/40G Network Module Ports	Yes	For small scale deployments (3850 fiber versions)	Yes
Catalyst 4500-E Series	Supervisor 8-E	Supervisor Uplink Ports	Yes	No	No
Catalyst 9300 Series	–	Onboard Ports and 10G/40G/mG Network Module Ports	Yes	No	No
Catalyst 9400 Series	Supervisor Engine-1	Supervisor and Line Card Ports	Yes	No	No
Catalyst 6807-XL Switch and Catalyst 6500-E Series	Supervisor 6T and Supervisor 2T	Supervisor Uplink Ports (Supervisor 6T Only) C6800 10G Series WS-X6900 Series	No	For existing topologies (requires DHCP server scope assignment policies)	Yes
Catalyst 6880-X and 6840-X Series	–	Onboard Ports and Port Card Ports	No	For existing topologies (requires DHCP server scope assignment policies)	Yes
Nexus 7700 Series	Supervisor 2E	M3 Series	No	For large scale 40G/100G deployments (requires DHCP server scope assignment policies)	No (requires manual configuration of dedicated external control plane node)
Catalyst 9500 Series	–	Onboard Ports	No	Yes	Yes

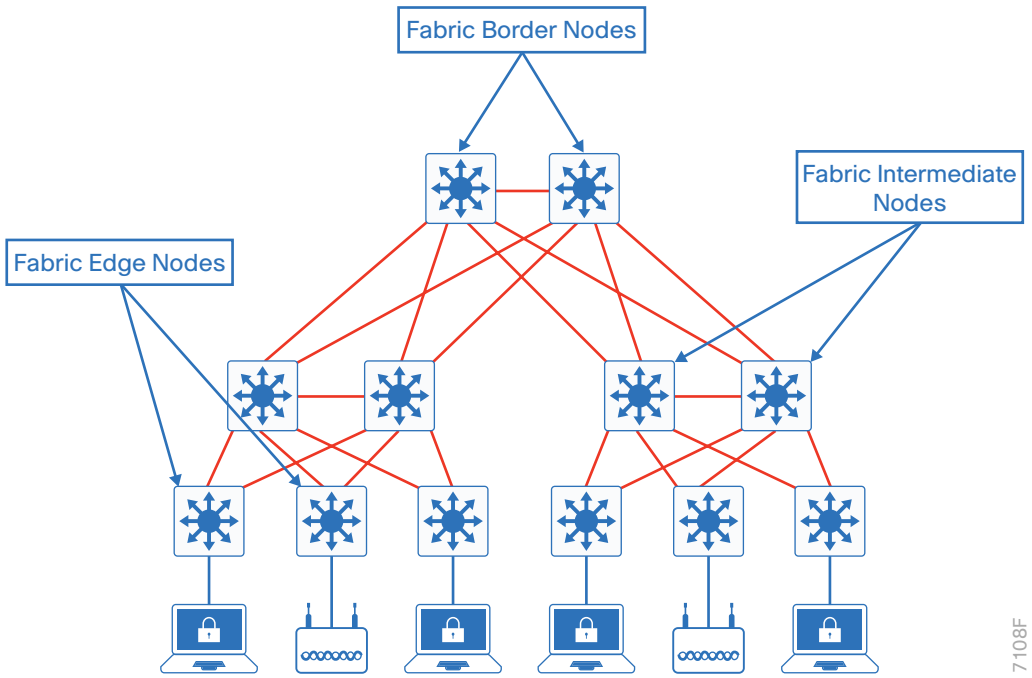
Table 2 SD-Access routing/wireless platforms and deployment recommendations

Platform	Supported Fabric-facing Interfaces	Recommended as Edge Node	Recommended as Border Node	Recommended as Control Plane Node
Cloud Services Router 1000V Series	–	–	–	Yes
Cisco 4000 Series Integrated Services Routers (ISR 4450/4430 for SD-Access 1.0)	Onboard LAN Ports and Routed LAN Network Interface Module and Enhanced Service Module Ports	No	Yes	No
Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers	Onboard LAN Ports, Ethernet Line Cards, and Ethernet Shared Port Adapters	No	Yes	Yes (large scale deployments)
8540, 5520, and 3504 Series Wireless Controllers	Via associated 802.11AC Wave 2 and Wave 1 Fabric Mode AP Network Ports	No	No	Proxy to Control Plane for Wireless Clients

PHYSICAL TOPOLOGIES

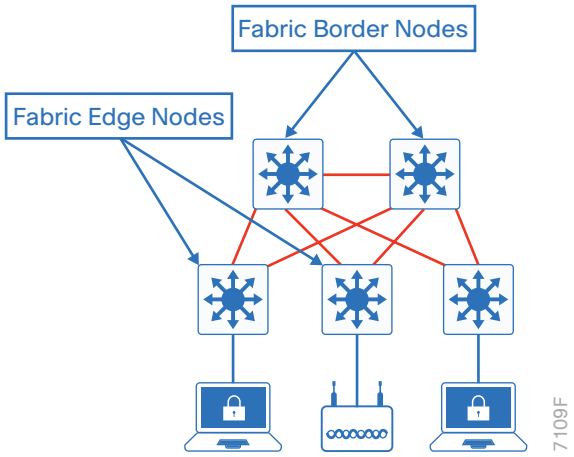
SD-Access topologies should follow the same design principles and best practices associated with a hierarchical design by splitting the network into modular groups. You create design elements that can be replicated throughout the network by using modular designs. The following example shows the physical topology of a three-tier campus design in which all nodes are dual homed with equal-cost links that will provide for load-balancing, redundancy, and fast convergence. Though the topology depicts the border at a campus core, the border can be configured separate from the core at another aggregation point. A cross link at each aggregation layer is used for optimal routing in case of an uplink failure.

Figure 7 Three-tier SD-Access fabric topology



For smaller deployments, an SD-Access fabric can be implemented using a two-tier design. The same design principles should be applied but without the need for an aggregation layer implemented by intermediate nodes.

Figure 8 *Two-tier SD-Access fabric topology*



SD-Access topologies should be deployed as spoke networks with the fabric border node at the exit point hub for the spokes, although other physical topologies can be used. Topologies in which the fabric is a transit network should be planned carefully in order to ensure optimal forwarding. If the border node is implemented at a node that is not the aggregation point for exiting traffic, sub-optimal routing results when traffic exits the fabric at the border and then doubles back to the actual aggregation point.

UNDERLAY NETWORK DESIGN

Having a well-designed underlay network will ensure the stability, performance, and efficient utilization of the SD-Access network. Automation for deploying the underlay is available using DNA Center.

Underlay networks for the fabric have the following design requirements:

- **Increase default MTU—**The VXLAN header adds 50 and optional 54 bytes of encapsulation overhead. Some Ethernet switches support a maximum transmission unit (MTU) of 9216 while others may have an MTU of 9196 or smaller. Given that server MTUs typically go up to 9,000 bytes, enabling a network wide MTU of 9100 ensures that Ethernet jumbo frames can be transported without any fragmentation inside and outside of the fabric.
- **Layer 3 to the access design—**The use of a Layer 3 routed network for the fabric provides the highest level of availability without the need to use loop avoidance protocols or interface bundling techniques.
- **Use point-to-point links—**Point-to-point links provide the quickest convergence times because they eliminate the need to wait for the upper layer protocol timeouts typical of more complex topologies. Combining point-to-point links with the recommended physical topology design provides fast convergence after a link failure. The fast convergence is a benefit of quick link failure detection triggering immediate use of alternate topology entries preexisting in the routing and forwarding table. Implement the point-to-point links using optical technology and not copper, because optical interfaces offer the fastest failure detection times to improve convergence.
- **Dedicated IGP process for the fabric—**The underlay network of the fabric only requires IP reachability from the fabric edge to the border node. In a fabric deployment, a single area IGP design can be implemented with a dedicated IGP process implemented at the SD-Access fabric. Address space used for links inside the fabric does not need to be advertised outside of the fabric and can be reused across multiple fabrics.
- **Loopback propagation—**The loopback addresses assigned to the underlay devices need to propagate outside of the fabric in order to establish connectivity to infrastructure services such as fabric control plane nodes, DNS, DHCP, and AAA. As a best practice, use /32 host masks. To propagate the loopback host routes, use route tags in order to enable an easy mechanism for redistributing only the loopbacks, to avoid maintaining prefix lists.

UNDERLAY AUTOMATION

You can fully automate the configuration of the underlay by using Cisco Network Plug and Play services in DNA Center. In non-greenfield deployment cases, you manually create the underlay. Manual underlays allow variations from the automated underlay deployment (for example, a different IGP could be chosen), but the previously listed underlay design principles still apply.

To automate the deployment of the underlay, DNA Center uses IP to access a seed device directly connected to the new underlay devices. The remaining devices are accessed using hop-by-hop CDP discovery and provisioning.

Tech Tip

The SD-Access 1.0 solution supports underlay automation using Catalyst 3850/3650 and Catalyst 9000 Series switches. For other platforms, see the release notes for your software version in order to verify support.

OVERLAY FABRIC DESIGN

In the SD-Access fabric, the overlay networks are used for transporting user traffic within the fabric. The fabric encapsulation also carries scalable group information that can be used for traffic segmentation inside the overlay. The following design considerations should be taken into account when deploying virtual networks:

- **Virtualize as needed for network requirements**—Segmentation using SGTs allows for simple-to-manage group-based policies and enables granular data plane isolation between groups of endpoints within a virtualized network, accommodating many network policy requirements. You can start with a default LAN fabric or create your unique set of virtual networks—VNs support the transport of SGTs for group segmentation. Use virtual networks when requirements dictate isolation at both the data plane and control plane. For those cases, if communication is required between different virtual networks, you use an external firewall or other device to enable inter-VN communication.
- **Reduce subnets and simplify DHCP management**—In the overlay, IP subnets can be stretched across the fabric without flooding issues that can happen on large Layer 2 networks. Use fewer subnets and DHCP scopes for simpler IP addressing and DHCP scope management.
- **Avoid overlapping IP subnets**—Different overlay networks can support overlapping address space, but be aware that most deployments require shared services across all VNs and other inter-VN communication. Avoid overlapping address space so that the additional operational complexity of adding a network address translation device is not required for shared services and inter-VN communication.

FABRIC CONTROL PLANE DESIGN

The fabric control plane node contains the database used to identify endpoint location for the fabric elements. This is a central and critical function for the fabric to operate. A control plane that is overloaded and slow to respond results in application traffic loss on initial packets. If the fabric control plane is down, endpoints inside the fabric fail to establish communication to remote endpoints that do not already exist in the local database.

DNA Center automates the configuration of the control plane functionality. For redundancy, you should deploy two control plane nodes to ensure high availability of the fabric, with the load distributed across both nodes. The devices supporting the control plane should be chosen to support the HTDB, CPU, and memory needs for an organization's needs.

FABRIC BORDER DESIGN

The fabric border design is dependent on how the fabric is connected to the outside network. VNs inside the fabric should map to VRF-Lite instances outside the fabric. Depending on where shared services are placed in the network the border design will have to be adapted. For more information, see "End-to-End Virtualization Considerations," later in this guide.

INFRASTRUCTURE SERVICES

SD-Access does not require any changes to existing infrastructure services, with the exception of the DHCP server for some default border configurations. In a typical DHCP relay design, the unique gateway IP address determines the subnet address assignment for an endpoint, in addition to the location where the DHCP server should direct the offered address. In a fabric overlay network, that gateway is not unique—the same Anycast IP address exists across all fabric edge devices within an overlay. Without special handling either at the border or by the DHCP server itself, the DHCP offer returning from the DHCP server through the border may not be relayed to the correct fabric edge switch where the DHCP request originated.

To identify the specific DHCP relay source, you use DHCP option 82 with the information option for circuit ID insertion on the relay agent at the fabric edge. Adding the information provides additional sub-options to identify the specific source relay agent. DHCP relay information embedded in the circuit ID is used as the destination for DHCP offer replies to the requestor—either by a fabric border with advanced DHCP border relay capabilities or, alternatively, by the DHCP server itself.

Using a border with the advanced DHCP border relay capability allows DHCP server scope configuration for fabrics to remain unchanged from standard non-fabric creation. When you are using border nodes with this capability, the borders inspect the DHCP offers returning from the DHCP server. The border node receiving the DHCP offer references the embedded circuit ID and directs the DHCP offers to the correct relay destination.

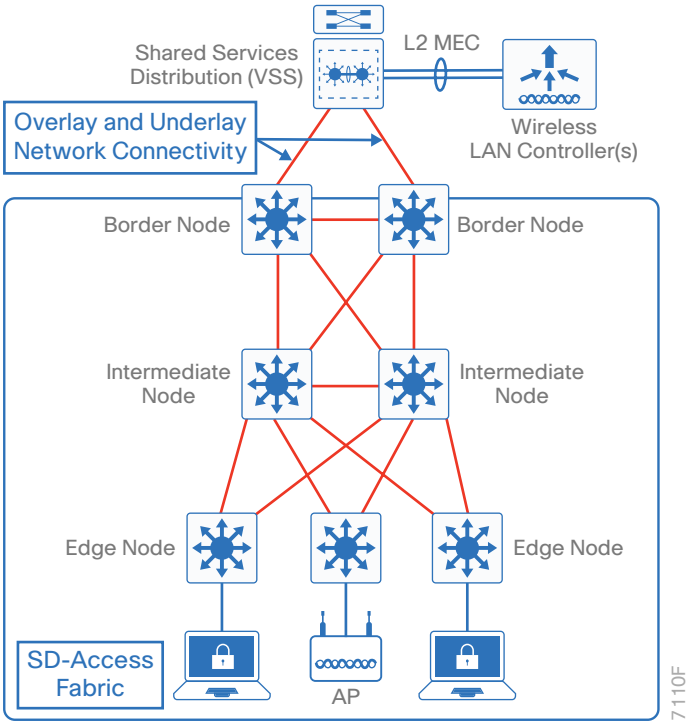
If you use a border without the advanced DHCP border relay capabilities, you modify the DHCP server itself to enable DHCP offers to be directed to the specific relay of the requestor. DHCP server scope selection criteria must be configured to reference the DHCP option 82 circuit ID information during offer creation to include the specific response destination. For information about implementing the DHCP server scopes, DHCP options, and selection criteria, refer to SD-Access deployment guides.

FABRIC WIRELESS INTEGRATION

As described earlier, when you integrate a fabric WLC and fabric mode APs into the SD-Access architecture, fabric WLCs are not active participants in the data plane traffic-forwarding role, and fabric mode APs are responsible for delivering wireless client traffic into and out of the wired fabric. The WLC control plane still keeps many of the characteristics of a local-mode controller, including the requirement to have a low-latency connection between the WLC and the APs. The colocation requirement precludes a fabric WLC from being the controller for fabric mode APs at a remote site across a typical WAN. As a result, a remote site desiring SD-Access with integrated wireless needs to have a local controller at that site.

When integrating wireless into SD-Access, another consideration is fabric WLC placement and connectivity. In larger scale deployments, typically WLCs are connected to a shared services distribution block that is part of the underlay. The preferred distribution block has chassis redundancy and also the capability to support L2 multi-chassis Etherchannel connections for link and platform redundancy to the WLCs. Often Virtual Switching System or switch-stacking is used to accomplish these goals. Because there is a need for the WLCs to connect to both the underlay and to the fabric overlay networks, virtualization (VRFs) must be extended from the border nodes through any infrastructure to the WLC connections. This topic is discussed in more detail in the Virtualization Technologies section.

Figure 9 *Wireless components integrated into SD-Access*



NON-FABRIC CENTRALIZED WIRELESS OPTION

In cases where you cannot dedicate WLCs and APs in a seamless roaming area to participate in fabric, a traditional CUWN design model, also known as a *local-mode model*, is an option. SD-Access is compatible with CUWN "over the top" as a non-native service option, without the benefits of fabric integration and DNA Center automation.

An over-the-top centralized design still provides IP address management, simplified configuration and troubleshooting, and roaming at scale. In a centralized model, the WLAN controller and APs are both located within the same site. You can connect the WLAN controller to a data center services block or a dedicated block off of the campus core. Wireless traffic between WLAN clients and the LAN is tunneled by using the control and provisioning of wireless access points (CAPWAP) protocol between the controller and the AP. APs can reside inside or outside the fabric without any change to the recommended centralized WLAN design.

For additional information about campus wireless design, see the Campus LAN and Wireless LAN Design Summary.

Tech Tip

In the SD-Access 1.0 solution, Converged Access and FlexConnect are not supported inside the SD-Access fabric.

SECURITY/POLICY DESIGN

Security policies vary by organization—it is not possible to define one-size-fits-all security design. Security designs are driven by information security policies and legal compliance. The planning phase for a security design is key to ensuring the right balance of security and user experience. You should consider the following aspects designing your security policy for the SD-Access network:

- **Openness of the network—**Some organizations allow only organization-issued devices in the network, and some support a "Bring Your Own Device" approach. Alternatively, you can balance user choice and allow easier-to-manage endpoint security by deploying a "Choose Your Own Device" model in which a list of IT-approved endpoints is offered to the users for business use. And an identity-based approach is also possible in which the network security policies can be deployed depending of the device ownership. For example, organization-issued devices may get group-based access, while personal devices may get Internet access only.
- **Identity management—**In the simplest form, identity management can be a username and password used for authenticating users. Adding embedded security functions and application visibility in the network devices provides telemetry for advanced policy definitions that can include additional context such as physical location, device used, type of access network, application used, and time of day.
- **Authentication, Authorization, and Accounting policies—***Authentication* is the process of establishing and confirming the identity of a client requesting access to the network. *Authorization* is the process of authorizing the endpoint to some set of network resources. Segmentation policies do not necessarily have to be enforced at the access layer, and can be deployed in multiple locations. Policies are enforced with the use of SGACLs for segmentation within VNs, and dynamic VLAN assignment for mapping endpoints into VNs at the fabric edge node.
- **Endpoint security—**Endpoints can be infected with malware, compromising data and create network disruptions. Malware detection, endpoint management, and data exports from the network devices provide insight into endpoint behavior. Tight integration of the network with security appliances and analytics platforms enable the network with the necessary intelligence to quarantine and help remediate compromised devices.
- **Data integrity and confidentiality—**Network segmentation can be used to control access to applications; encryption of the data path in the switching environment using IEEE 802.1AE is used to provide encryption at Layer 2 to prevent eavesdropping and to ensure that the data cannot be modified.
- **Network device security—**Hardening the security of the network devices is essential because they are common targets for security attacks. The use of the most secure device management options, such as enabling device authentication using TACACS+ and disabling unnecessary services, are best practices to ensure the network devices are secured.

Enabling group-based segmentation within each VN allows for simplified hierarchical network policies. Network-level policy scopes of isolated control and data planes are possible using VNs, and group-level policy scopes are possible using SGTs within VNs, enabling common policy application across the wired and wireless fabric.

SGTs provide the capability to tag endpoint traffic based on a role or function within the network and subject to role-based policies or SGACLs centrally defined at ISE. In most deployments, Active Directory is used as the identity store for user accounts, credentials, and group membership information. Upon successful authorization, endpoints can be classified based on that information and assigned the appropriate scalable group assignments. These scalable groups can then be used to create segmentation policies and virtual network assignment rules.

SGT information is carried across the network in several forms:

- **Inside the SD-Access network—**The SD-Access fabric header transports SGT information. Fabric edge nodes and border nodes can enforce SGACLs to enforce the security policy.
- **Outside of the fabric on a TrustSec-capable device—**Inline TrustSec-capable devices carry the SGT information in a CMD header on the Layer 2 frame. This is the recommended mode of transport outside of the SD-Access network.
- **Outside of the fabric over devices without TrustSec capability—**SXP allows the transport of SGTs over a TCP connection. This can be used to bypass network devices that do not support SGT inline.

For additional information about Cisco TrustSec, see www.cisco.com/go/trustsec.

DESIGN SCALE CONSIDERATIONS

In addition to the platform role recommendations listed in Table 1, consider the following scaling parameters when designing SD-Access for an organization.

Tech Tip

The numbers listed are maximum limits supported in the SD-Access 1.0 solution. Check hardware and software release notes for additional limits of specific components.

Table 3 DNA Center Maximum Scale Constraints

SD-Access Construct	Maximum for Single DNA Center	Maximum per Fabric Domain
Endpoints (wired/wireless)—Across all Fabric Domains	20,000	20,000
Endpoints per Fabric Edge Node	5,000	5,000
Fabric Nodes—Across all Fabric Domains (Routers, Switches/Switch Stacks, WLCs)	2,500	500
Access Points—Across all Fabric Domains (each AP counts as an endpoint)	2,500	–
IP Pools—Across all Fabric Domains	500	500
Sites	500	–
Fabric Domains	10	–
Scalable Group Tags—Across all Fabric Domains	4,000	1,000
Policies—Across all Fabric Domains	1,000	–
Contracts—Across all Fabric Domains	500	–
Control Plane Nodes	–	2
Default Border Nodes	–	2

Table 4 SD-Access Edge Node Scale Constraints

	Catalyst 3850/3650	Catalyst 9300	Catalyst 4500 Supervisor 8-E	Catalyst 9400 Supervisor Engine-1
Virtual Networks	64	256	64	256
Scalable Group Tags	4,000	8,000	2,000	8,000
Security Group ACLs	1,500	5,000	64,000	18,000

Table 5 SD-Access Border Node Scale Constraints

	Catalyst 3850 (Fiber)	Catalyst 9500	Catalyst 6800	Nexus 7700 Supervisor 2E	ASR 1000 and ISR 4000
Virtual Networks	64	256	512	500	4,000
Scalable Group Tags	4,000	32,000	30,000	64,000	64,000
Security Group ACLs	1,500	32,000	30,000	64,000	64,000
IP to SGT Mappings	2,000	32,000	30,000	64,000	64,000
Fabric Control Plane Entries	4,000	96,000	25,000	Unsupported	200,000
IPv4 Routes	8,000	48,000	48,000	1,000,000 (XL) 256,000 (non-XL)	4,000,000 (16GB) 1,000,000 (8GB)
IPv4 Host Entries	16,000	96,000	48,000	1,000,000 (XL) 256,000 (non-XL)	4,000,000 (16GB) 1,000,000 (8GB)

End-to-End Design Considerations

In a virtualized network, there is full isolation of data and control planes over a shared networking infrastructure. In the case of the SD-Access, a user on one VN is completely isolated and will not be able to communicate with a user on a different VN. The fabric border node is responsible for extending network virtualization beyond the SD-Access fabric. Organizations may have business requirements that call for this type of isolation. Some example of vertical specific use cases where network virtualization maybe useful include:

- **Education**—College campus divided into administrative and student residence networks.
- **Retail**—Isolation for point-of-sale machines supporting payment card industry compliance.
- **Manufacturing**—Isolation for machine-to-machine traffic in manufacturing floors.
- **Healthcare**—Dedicated networks for medical equipment, patient guest access and HIPAA compliance.
- **Enterprise**—Integration of networks during mergers, where overlapping address spaces may exist. Separation of building control systems and video surveillance devices.

Designing for end-to-end network virtualization requires detailed planning in order to ensure the integrity of the virtual networks. In most cases, there is a need to have some form of shared services that can be reused across multiple virtual networks. It is important that those shared services are deployed correctly in order to preserve the isolation between different virtual networks sharing those services. The use of a fusion router directly attached to the fabric border provides a mechanism for route leaking shared services prefixes across multiple networks, the use of firewalls provides an additional layer of security and monitoring of traffic between virtual networks. Examples of shared services include:

- **Wireless infrastructure**—Radio frequency performance and cost efficiency is increased using common wireless LANs (single SSID). Traffic isolation is achieved by assigning dedicated VLANs at the WLC and using dynamic VLAN assignment using 802.1X authentication to map wireless endpoints into their corresponding VNs.
- **DHCP, DNS, and IP address management**—The same set of infrastructure services can be reused as long as they have support for virtualized networks. Special capabilities such as advanced DHCP scope selection criteria, multiple domains, and support for overlapping address space are some of the capabilities required to extend the services beyond a single network.
- **Internet access**—The same set of Internet firewalls can be used for multiple virtual networks. If firewall policies need to be unique for each virtual network, the use of a multi-context firewall is recommended.
- **IP communications**—When IP phones and other unified communications devices are connected in multiple virtual networks, the call control signaling to the communications manager and the IP traffic between those devices needs to be able to traverse multiple VNs in the infrastructure.

NETWORK VIRTUALIZATION TECHNOLOGIES

Extending the SD-Access fabric virtualization beyond the fabric border is enabled using multi-VRF configurations. SD-Access VNs can have 1:1 or N:1 mapping to VRFs outside of the SD-Access fabric. Guidance for virtualizing your end-to-end network is beyond the scope of this guide. However, this section provides a brief introduction to the most commonly used technologies that you can investigate when virtualizing your network.

Device Level Virtualization

Within the same device physical device, logical separation capabilities at Layer 2 and Layer 3 can be used to extend virtual networks:

Virtual LANs

The most basic form of device-level virtualization is isolating network traffic using different virtual LANs (VLANs). This form of virtualization applies to Layer 2 devices and can be extended across switched domains. VLANs are also used to virtualize point-to-point links between routers and security appliances that require connectivity to multiple virtual networks via the same physical interface.

Virtual Routing and Forwarding

VRF is a device-level virtualization technology for creating multiple Layer 3 routing tables on the same device. VRFs can be tied to existing Layer 2 domains in order to provide Layer 3 edge functionality to multiple VLANs and also between Layer 3 routed interfaces in order to extend a multiple virtualized control plane over the same set of interfaces.

Path Isolation

To maintain isolation on the paths of links interconnecting devices, there are many technology options that provide network virtualization among devices. For SD-Access, the recommended path-isolation technologies are VRF-Lite and MPLS VPN. The number of virtualized networks required typically dictates the design. If you forecast a need for more than a few VRFs, deploying MPLS VPNs simplifies configuration and management.

VRF-Lite End-to-End

VRF-Lite is deployed on a hop-by-hop basis in a campus network, making use of 802.1Q trunks between devices in order to isolate data and control plane for each virtual network. For ease of operation, you should use the same set of VLANs across every hop and use BGP with per-VN address families providing attributes that can be leveraged for easy route-leaking for shared services.

MPLS

Although often considered a service-provider technology, MPLS is common on larger enterprises needing a large number of virtualized networks, most commonly in the WAN but also extended to the campus network. While VRF-Lite is common to most routing platforms, MPLS is not supported across all platforms. A combination of VRF-Lite at the edge with MPLS VPN is another design that could be considered.

Tech Tip

The SD-Access 1.0 solution supports VRF-Lite handoff at the fabric border node. For other options, reference the release notes for your software version to verify support.

Migration to SD-Access

You can readily create SD-Access greenfield networks by adding the infrastructure components, interconnecting them, and using DNA Center with Cisco Plug and Play features to automate provisioning of the network architecture from the ground up. Migrating an existing network requires some additional planning. Here are some example considerations:

- Migration typically implies that a manual underlay is used. Does an organization's underlay network already include the elements described in the "Underlay Network" section? Or do you have to reconfigure your network into a Layer 3 access model?
- Do the SD-Access components in the network support the desired scale for the target topologies, or do the hardware and software platforms need to be augmented with additional platforms?
- Is the organization ready for changes in IP addressing and DHCP scope management?
- If you plan to enable multiple VNs, what is the strategy for integrating those VNs with common services (for example: Internet, DNS/DHCP, data center applications)?
- Are SGTs already implemented, and where are the policy enforcement points? If SGTs and multiple VNs are used to segment and virtualize within the fabric, what requirements for extending them beyond the fabric exist? Is infrastructure in place to support TrustSec, VRF-Lite, MPLS, fusion routers or other technologies necessary to extend and support the segmentation and virtualization?
- Can wireless coverage within a roaming domain be upgraded at a single point in time, or do you need to rely on over-the-top strategies?

There are two primary approaches when migrating an existing network to SD-Access. If many of the existing platforms are to be replaced, and if there is sufficient power, space, and cooling, then building an SD-Access network in parallel may be an option allowing for easy user cutovers. Building a parallel network that is integrated with the existing network is effectively a variation of a greenfield build. Another approach is to do incremental migrations of access switches into an SD-Access fabric. This strategy is appropriate for networks that have equipment capable of supporting SD-Access already in place or where there are environmental constraints.

For detailed coverage of migration topics, see Software-Defined Access Migration on cisco.com.

Appendix–Glossary

AAA authentication, authorization, and accounting

ACL access control list

AP access point

BGP border gateway protocol

CAPWAP control and provisioning of wireless access points protocol

CMD Cisco Meta Data

DNA Cisco Digital Network Architecture

EID endpoint identifier

HTDB host tracking database

IGP interior gateway protocol

ISE Cisco Identity Services Engine

LISP Locator/ID Separation Protocol

MR Map-Resolver

MS Map-Server

MTU maximum transmission unit

RLOC routing locator

SD-Access Software-Defined Access

SGACL scalable group access control list

SGT scalable group tag

SXP scalable group tag exchange protocol

VLAN virtual local area network

VN virtual network

VNI virtual extensible LAN network identifier

VRF virtual routing and forwarding

VTEP virtual extensible LAN tunnel endpoint

VXLAN virtual extensible LAN

You can use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.