Software-Defined Access

Solution Design Guide

September, 2019
Contents

Cisco Digital Network Architecture and Software-Defined Access 3
SD-Access Solution Components 5
Software-Defined Access Architecture 12
Cisco SD-Access Site Reference Models 24
Migration to SD-Access 41
Appendix A—SD-Access Fabric Protocols 42
Appendix B—Glossary 44
Feedback 45
Cisco Digital Network Architecture and Software-Defined Access

Cisco® Software-Defined Access (SD-Access) is the evolution from traditional campus LAN designs to networks that directly implement the intent of an organization. SD-Access is enabled with an application package that runs as part of the Cisco DNA Center software for designing, provisioning, applying policy, and facilitating the creation of an intelligent campus wired and wireless network with assurance.

Fabric technology, an integral part of SD-Access, provides wired and wireless campus networks with programmable overlays and easy-to-deploy network virtualization, permitting a physical network to host one or more logical networks as required to meet the design intent. In addition to network virtualization, fabric technology in the campus network enhances control of communications, providing 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 for scalable groups within a virtual network using scalable group tags (SGTs). Using Cisco DNA Center to automate the creation of virtual networks reduces operational expenses, coupled with the advantage of reduced risk, with integrated security and improved network performance provided by the assurance and analytics capabilities.

This design 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. It is a companion to the associated deployment guides for SD-Access, which provide configurations explaining how to deploy the most common implementations of the designs 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.

If you didn’t download this guide from Cisco Community or Design Zone, you can check for the latest version of this guide.


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

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 to react quickly to application demands and growth. Because the campus LAN is the network within a location that people and devices use to access applications, the campus wired and wireless LAN capabilities should be enhanced to support those changing needs.

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

Flexible Ethernet foundation for growth and scale

- **Simplified deployment and automation**—Network device configuration and management through a centralized controller using open APIs allows for very fast, lower-risk deployment of network devices and services.
- **Increased bandwidth needs**—Bandwidth needs are doubling potentially multiple times over the lifetime of a network, resulting in the need for new networks to aggregate using 10 Gbps Ethernet to 40 Gbps to 100 Gbps capacities over time.
- **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
Gb/s 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, such as lighting, surveillance cameras, virtual desktop terminals, remote access switches, and APs, may require higher power to operate. 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 Power over Ethernet (PoE) perpetual power during switch upgrade and reboot events. The Cisco Catalyst 9000 family of access layer switches is perpetual PoE-capable and hardware-ready for 100W per port, as that technology becomes available.

### Integrated services and 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-related 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 access and application 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 assigned from group-based policies can be used to segment a network 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 different sets of users and applications to be isolated securely.

### SD-Access Use Case for Healthcare Networks: Secure Segmentation & Profiling

Our healthcare records are just as valuable to attackers as our credit card numbers and online passwords. In the wake of recent cyber-attacks, hospitals are required to have HIPAA-compliant wired and wireless networks that can provide complete and constant visibility into their network traffic to protect sensitive medical devices (such as servers for electronic medical records, vital signs monitors, or nurse workstations) so that a malicious device cannot compromise the networks.

A patient’s mobile device, when compromised by malware, can change network communication behavior to propagate and infect other endpoints. It is considered abnormal behavior when a patient’s mobile device communicates with any medical device. SD-Access can address the need for complete isolation between patient devices and medical facility devices by using macro-segmentation and putting devices into different overlay networks, enabling the isolation.

How is a similar scenario addressed for the case of a compromised medical professional’s mobile device requiring connectivity to information systems for some tasks, but not requiring connectivity to other medical devices? SD-Access can take this need for segmentation beyond simple network separation by profiling devices and users as they come onto the network and applying micro-segmentation within an overlay network. Flexible policy creation provides the ability to have groups of device types and user roles, to restrict communication within a group, or to enable communication among groups only as needed to implement the intent of the policies of an organization.

Deploying the intended outcomes for the needs of the organization is simplified by using the automation capabilities built into Cisco DNA Center, and those simplifications span the wired and wireless domains.
Other organizations may have business requirements where secure segmentation and profiling are needed similar to Healthcare:

- **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 wireless 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.

**SD-Access Solution Components**

The SD-Access solution combines the Cisco DNA Center software, identity services, and wired and wireless fabric functionality. Within the SD-Access solution, a fabric site is composed of an independent set of fabric control plane nodes, edge nodes, intermediate (transport only) nodes, and border nodes. Wireless integration adds fabric WLC and fabric mode AP components to the fabric site. Fabric sites can be interconnected using different types of transit networks like IP Transit, SDWAN Transit (future) and SD-Access transit network to create a larger fabric domain. This section describes the functionality for each role; how the roles map to the physical campus topology; the components required for solution management, wireless integration, and policy application.
**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 database tracks all endpoints in the fabric site and associates the endpoints to fabric nodes, decoupling the endpoint IP address or MAC address from the location (closest router) in the network. The control plane node functionality can be collocated with a border node or can use dedicated nodes for scale, and between two and six nodes (for wired deployments only) are used for resiliency. Border and edge nodes register with and use all control plane nodes, so resilient nodes chosen should be of the same type for consistent performance.

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 LAN design. The edge nodes implement a Layer 3 access design with the addition of the following fabric functions:

- **Endpoint registration**—Each edge node has a LISP control-plane session to all control plane nodes. 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 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. An SGT is also assigned, and an SGT can be used to provide segmentation and policy enforcement at the fabric edge.

<table>
<thead>
<tr>
<th>Tech tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS® Software enhances 802.1X device capabilities with Cisco Identity Based Networking Services (IBNS) 2.0. For example, concurrent authentication methods and interface templates have been added. Likewise, Cisco DNA Center has been enhanced to aid with the transition from IBNS 1.0 to 2.0 configurations, which use Cisco Common Classification Policy Language (commonly called C3PL). See the release notes and updated deployment guides for additional configuration capabilities. For more information about IBNS, see: <a href="https://cisco.com/go/ibns">https://cisco.com/go/ibns</a>.</td>
</tr>
</tbody>
</table>

- **Anycast Layer 3 gateway**—A common gateway (IP and MAC addresses) can be used at every node that shares a common EID subnet providing optimal forwarding and mobility across different RLOCs.

- **LISP forwarding**—Instead of a typical routing-based decision, the fabric edge nodes query the map server to determine the RLOC associated with the destination EID and use that information as the traffic destination. 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 Cisco Express Forwarding table and installed in hardware. If 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 to trigger a new map request; this addresses the case where the endpoint may be present on a different fabric edge switch.

- **VXLAN encapsulation/de-encapsulation**—The fabric edge nodes use the RLOC associated with the destination IP address to encapsulate the traffic with VXLAN headers. Similarly, VXLAN traffic received at a destination RLOC is de-encapsulated. The encapsulation and de-encapsulation of traffic enables the location of an endpoint to change and be encapsulated with a different edge node and RLOC in the network, without the endpoint having to change its address within the encapsulation.

**Intermediate node**

The fabric intermediate nodes are part of the Layer 3 network used for interconnections among the edge nodes to the border nodes. In the case of a three-tier campus design using core, distribution, and access layers, the intermediate nodes are the equivalent of distribution switches, although the number of intermediate nodes is not limited to a single layer of devices. Intermediate nodes route and transport IP traffic inside the fabric. No VXLAN encapsulation/de-encapsulation, LISP control plane messages, or SGT awareness requirements exist on an intermediate node, which has only the additional fabric MTU requirement to accommodate the larger-size IP packets encapsulated with VXLAN information.

**Border node**

The fabric border nodes serve as the gateway between the SD-Access fabric site and the networks external to the fabric. The fabric border node is responsible for network virtualization interworking and SGT propagation from the fabric to the rest of the network. Most networks use an external border, for a common exit point from a fabric, such as for the rest of an enterprise
network along with the Internet. The external border is an efficient mechanism to offer a default exit point to all virtual networks in the fabric, without importing any external routes. A fabric border node has the option to be configured as an internal border, operating as the gateway for specific network addresses such as a shared services or data center network, where the external networks are imported into the VNs in the fabric at explicit exit points for those networks. A border node can also have a combined role as an anywhere border (both internal and external border), which is useful in networks with border requirements that can't be supported with only external borders, where one of the external borders is also a location where specific routes need to be imported using the internal border functionality.

- Border nodes implement the following functions:
  - **Advertisement of EID subnets**—SD-Access configures border gateway protocol (BGP) as the preferred routing protocol used to advertise the EID prefixes outside the fabric, and traffic destined for EID subnets coming in 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.
  - **Fabric domain exit point**—The external 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 internal 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 with VRF-aware routing protocols 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. SGT information is propagated from the fabric border node to the network external to the fabric, either by transporting the tags to Cisco TrustSec-aware devices using SGT Exchange Protocol (SXP) or by directly mapping SGTs into the Cisco metadata field in a packet, using inline tagging capabilities implemented for connections to the border node.

**Extended node**

You can extend fabric capabilities to Cisco Industrial Ethernet switches, such as the Cisco Catalyst Digital Building Series and Industrial Ethernet 3000, 4000, and 5000 Series, by connecting them to a Cisco Catalyst 9000 Series SD-Access fabric edge node, enabling segmentation for user endpoints and IoT devices.

Using Cisco DNA Center automation, switches in the extended node role are connected to the fabric edge using an 802.1Q trunk over an EtherChannel with one or multiple physical members and discovered using zero-touch Plug-and-Play. Endpoints, including fabric-mode APs, connect to the extended node switch. VLANs and SGTs are assigned using host onboarding as part of fabric provisioning. Scalable group tagging policy is enforced at the fabric edge.

The benefits of extending fabric capabilities using extended nodes are operational IoT simplicity using Cisco DNA Center-based automation, consistent policy across IT and OT, and greater network visibility of IoT devices.

For more information on extended go to: [https://www.cisco.com/iot](https://www.cisco.com/iot)

**Fabric wireless LAN controller**

The fabric WLC integrates with 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 of the fabric control plane 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 to the fabric edges those SSIDs.
Typically, the fabric WLC devices connect to a shared services distribution or data center outside the fabric and fabric border, which means that their management IP address exists in the global routing table. For the wireless APs to establish a CAPWAP tunnel for WLC management, the APs must be in a VN that has access to the external device. In the SD-Access solution, Cisco DNA Center configures wireless APs to reside within the VRF named INFRA_VRF, which maps to the global routing table, avoiding the need for route leaking or fusion router (multi-VRF router selectively sharing routing information) services to establish connectivity. Each fabric site has to have a WLC unique to that site. It is recommended to place the WLC in the local site itself because of latency requirements for SD-Access. Latency will be covered in a section below in more detail.

Small- to medium-scale deployments of Cisco SD-Access can use the Cisco Catalyst 9800 Embedded Wireless Controller. The controller is available for the Catalyst 9300 Switch as a software package update to provide wired and wireless (fabric only) infrastructure with consistent policy, segmentation, security and seamless mobility, while maintaining the ease of operation of the Cisco Unified Wireless Network. The wireless control plane remains unchanged, using CAPWAP tunnels initiating on the APs and terminating on the Cisco Catalyst 9800 Embedded Wireless Controller. The data plane uses VXLAN encapsulation for the overlay traffic between the APs and the fabric edge.

The Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series software package enables wireless functionality only for Cisco SD-Access deployments with two supported topologies:

- Cisco Catalyst 9300 Series switches functioning as collocated border and control plane.
- Cisco Catalyst 9300 Series switches functioning as a fabric in a box.

The embedded controller only supports fabric mode access points.

**Fabric mode access points**

The fabric mode APs are Cisco WiFi6 (802.11ax) and 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 wireless media services that traditional APs support; apply AVC, quality of service (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. The fabric edge nodes use CDP to recognize APs as special wired hosts, applying special port configurations and assigning the APs to a unique overlay network within a common EID space across a fabric. The assignment allows management simplification by using a single subnet to cover the AP infrastructure at a fabric site.

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 Layer 2 VNI and an SGT supplied by ISE. Then the WLC registers the wireless client Layer 2 EID into the control plane, acting as a proxy for the egress fabric edge node switch. After the initial connectivity is established, the AP uses the Layer 2 VNI information to VXLAN-encapsulate wireless client communication on the Ethernet connection 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 a secure network access platform enabling increased management awareness, control, and consistency for users and devices accessing an organization’s network. 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. Within ISE, users and devices are shown in a simple and flexible interface. ISE integrates with Cisco DNA Center by using Cisco Platform Exchange Grid (pxGrid) and REST 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 Cisco 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 defined, managed, and administered by Cisco ISE. ISE and Cisco DNA Center are tightly integrated through REST APIs, with management of the policies driven by Cisco DNA Center.

ISE supports standalone and distributed deployment models. Additionally, multiple distributed nodes can be deployed together supporting failover resiliency. The range of options allows support for hundreds of thousands of endpoint devices, with a subset of the devices used for SD-Access to the limits described later in the guide. Minimally, a basic two-node ISE deployment is recommended for SD-Access deployments, with each node running all services for redundancy.

SD-Access fabric edge node switches send authentication requests to the Policy Services Node (PSN) persona running on ISE. In the case of a standalone deployment, with or without node redundancy, that PSN persona is referenced by a single IP address. An ISE distributed model uses multiple active PSN personas, each with a unique address. All PSN addresses are learned by Cisco DNA Center, and the Cisco DNA Center user maps fabric edge node switches to the PSN that supports each edge node.

**Cisco DNA Center**

At the heart of automating the SD-Access solution is Cisco DNA Center. SD-Access is enabled with an application package that runs as part of the Cisco DNA Center software for designing, provisioning, applying policy, and facilitating the creation of an intelligent campus wired and wireless network with assurance.

Cisco DNA Center centrally manages major configuration and operations workflow areas.

- **Design**—Configures device global settings, network site profiles for physical device inventory, DNS, DHCP, IP addressing, software image repository and management, device templates, and user access.

- **Policy**—Defines business intent for provisioning into the network, including creation of virtual networks, assignment of endpoints to virtual networks, policy contract definitions for groups, and configures application policies.

- **Provision**—Provisions devices and adds them to inventory for management, supports Cisco Plug and Play, creates fabric domains, control plane nodes, border nodes, edge nodes, fabric wireless, Cisco Unified Wireless Network wireless, transit, and external connectivity.

- **Assurance**—Enables proactive monitoring and insights to confirm user experience meets configured intent, using network, client, and application health dashboards, issue management, and sensor-driven testing.

- **Platform**—Allows programmatic access to the network and system integration with third-party systems using APIs, using feature set bundles, configurations, a runtime dashboard, and a developer toolkit.

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

- All controller functionality is exposed through northbound REST APIs.

- Organizations and ecosystem partners can easily build new applications.

- All northbound REST API requests are governed by the controller RBAC mechanism.

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

The Cisco DNA Center software, including the SD-Access application package, is designed to run on the Cisco DNA Center Appliance. The appliance is available in form factors sized to support not only the SD-Access application but also network assurance and new capabilities as they are available.

When you deploy a single Cisco DNA Center Appliance only, and then that appliance node becomes unavailable, an SD-Access network provisioned by the node still functions, but automated provisioning capabilities are lost until the single node availability is restored. For high-availability purposes, configure three Cisco DNA Center appliances of the same appliance type to form a three-node cluster. The Cisco DNA Center cluster is accessed using a single GUI interface hosted on a virtual IP, which is serviced by the resilient nodes within the cluster. Single nodes should be configured with future clustering in mind, to easily enable multi-node clustering, as required in the future.

Within a three-node cluster, you enable service distribution to automatically provide distributed processing, database replication, security replication, and file synchronization. Software upgrades are also automatically replicated across the nodes in a cluster. A cluster will survive the loss of a single host and requires two hosts to remain operational. Some maintenance operations, such as software upgrades and file restoration from backup, are restricted until the full three-node cluster is restored, and not all assurance data may be protected while in the degraded two-node state.

For provisioning and assurance communication efficiency, the Cisco DNA Center cluster should be installed in close network proximity to the greatest number of devices being managed, minimizing communication delay to the devices.

For additional information about the Cisco DNA Center Appliance capabilities, see the data sheet on Cisco.com.

Shared Services

Designing for end-to-end network virtualization requires detailed planning 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 to preserve the isolation between different virtual networks sharing those services. Examples of shared services include:

- **DHCP, DNS, and IP address management**—The same set of infrastructure services can be reused if 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 voice/video collaboration services**—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.
Software-Defined Access Architecture

The SD-Access architecture is supported by fabric technology implemented for the campus, enabling the use of virtual networks (overlay networks) running on a physical network (underlay network) creating alternative topologies to connect devices. Overlay networks in data center fabrics commonly are used to provide Layer 2 and Layer 3 logical networks with virtual machine mobility (examples: Cisco ACI™, VXLAN/EVPN, and FabricPath). Overlay networks also are 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 as well as design recommendations.

Underlay network
The underlay network is defined by the physical switches and routers that are used to deploy the SD-Access network. All network elements of the underlay must establish IP connectivity via the use of a routing protocol. Instead of using arbitrary network topologies and protocols, the underlay implementation for SD-Access uses a well-designed Layer 3 foundation inclusive of the campus edge switches (also known as a routed access design), to ensure performance, scalability, and high availability of the network.

In SD-Access, the underlay switches support the endpoint physical connectivity for users. However, end-user subnets and endpoints are not part of the underlay network—they are part of a programmable Layer 2 or Layer 3 overlay network.


Underlay network design considerations
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 Cisco DNA Center.

Underlay networks for the fabric have the following design requirements:

- **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.

- **Increase default MTU**—The VXLAN header adds 50 and optionally 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.

- **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.

- **ECMP**—Equal-cost multi-path routing is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple best paths. Load balancing between these ECMP paths is performed automatically using Cisco Express Forwarding (CEF). ECMP-aware IGP routing protocols should be used to take advantage of the parallel-cost links and to provide redundant forwarding paths for resiliency.

- **BFD**—Bidirectional Forwarding Detection should be used to enhance fault detection and convergence characteristics of IGPs.

- **NSF**—Non-stop forwarding works with SSO (stateful switchover) to provide continued forwarding of packets in the event of a route processor (RP) switchover. NSF-aware IGP routing protocols should be used to minimize the amount of time that a network is unavailable following a switchover.
- **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, typically using a link-state protocol, such as IS-IS, for performance advantages. While IS-IS is used for LAN Automation, other routing protocols such as OSPF and EIGRP are supported and are both ECMP and NSF-aware.

- **Loopback propagation**—The loopback addresses assigned to the underlay devices need to propagate outside of the fabric to establish connectivity to infrastructure services such as fabric control plane nodes, DNS, DHCP, and AAA. Use /32 host masks is required for RLOC reachability, and the default route cannot be used for this purpose. Apply tags to the host routes as they are introduced into the network. Reference the tags to redistribute and propagate only the tagged loopback routes. This is an easy way to selectively propagate routes outside of the fabric and avoid maintaining prefix lists.

- **WLC reachability**—Connectivity to the WLC should be treated like the loopback addresses. A default route in the underlay cannot be used by the APs to reach the WLCs. A specific route to the WLC IP address must exist in the Global Routing Table at each switch where the APs are physically connected.

- **LAN Automation for Deployment** - You can automate the configuration of the underlay by using LAN automation services in Cisco 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. The Cisco DNA Center LAN automation feature is an alternative to manual underlay deployments for new networks and uses an IS-IS routed access design. Although there are many alternative routing protocols, the IS-IS selection offers operational advantages such as neighbor establishment without IP protocol dependencies, peering capability using loopback addresses, and agnostic treatment of IPv4, IPv6, and non-IP traffic.

- In the latest versions of Cisco DNA Center, LAN automation uses Cisco Network Plug and Play features to deploy both unicast and source-specific multicast routing configuration in the underlay, aiding traffic delivery efficiency for the services built on top.

- Using LAN Automation to automate the network underlay provides orchestration of MTU, routed point-to-point links, ECMP, NSF, BFD, and routed access while also propagating the Loopback addresses for the automated fabric nodes. It also provisions CLI and SNMP credentials while using SWIM to upgrade the device software to the desired version.

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

**Latency considerations**

Fabric access points operate in local mode. This requires a RTT (round-trip time) of 20ms or less between the AP and the Wireless LAN Controllers. This generally means that the WLC is deployed in the same physical site as the Access Points. If dedicated dark fiber exists between the physical sites and the WLCs in the data center and the latency requirement is meant, WLCs and APs may be in different physical locations. This is commonly seen in metro area networks and SD-Access for Distributed Campus. APs should not be deployed across the WAN from the WLCs.

Cisco DNA Center 3-Node Clusters must have a RTT of 10ms or less between nodes in the cluster. For physical topology options and failover scenarios, please see Cisco DNA Center 3-Node Cluster High Availability scenarios and network connectivity details technote.

Latency in the network is an important consideration for performance and the RTT between Cisco DNA Center and any network device it manages should be taken into account. The optimal RTT should be less than 100 milliseconds to achieve optimal performance for Base Automation, Assurance, Software-Defined Access, and all other solutions provide by Cisco DNA Center.
The maximum supported latency is 200ms. Latency between 100ms and 200ms is supported, although longer execution times could be experienced for certain events including Inventory Collection, Fabric Provisioning, SWIM, and other processes.

**Figure 2. Cisco SD-Access Network Requirements**

**Cisco SD-Access Network Requirements**

**Overlay network**

An overlay network is created on top of the underlay to create a virtualized network. The data plane traffic and control plane signaling are contained within each virtualized network, maintaining isolation among the networks as well as independence from the underlay network. The SD-Access fabric implements virtualization by encapsulating user traffic in overlay networks using IP packets that are sourced and terminated at the boundaries of the fabric. The fabric boundaries include borders for ingress and egress to a fabric, fabric edge switches for wired clients, and fabric APs for wireless clients. 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 multitenancy through virtualization. Each overlay network appears as a virtual routing and forwarding (VRF) instance for connectivity to external networks. You preserve the overlay separation when extending the networks outside of the fabric by using VRF-lite, maintaining the network separation within devices connected to the fabric and on the links between VRF-enabled devices.

Layer 2 overlays emulate a LAN segment to transport Layer 2 frames, carrying a single subnet over the Layer 3 underlay. Layer 2 overlays are useful in emulating physical topologies and can be subject to Layer 2 flooding. By default, SD-Access supports transport of IP frames without Layer 2 flooding of broadcast and unknown multicast traffic, altering from the behavior and reducing restrictions of a traditional LAN to permit creation of larger subnetworks. The SD-Access Solution Components section describes the fabric components required to allow ARP to function without broadcasts from the fabric edge, accomplished by using the fabric control plane for MAC-to-IP address table lookups.
Layer 3 overlays abstract the IP-based connectivity from the physical connectivity and allow multiple IP networks as part of each virtual network.
In early versions of SD-Access, IPv4 multicast forwarding within the overlay operates using *headend replication* of multicast packets into the fabric for both wired and wireless endpoints, meaning that border (headend) must take each multicast packet, and for each edge receiver switch, replicate the packet and forward it. Recent versions of SD-Access have the option to use underlay multicast capabilities with many of the platforms, either configured manually or by using LAN automation, for more efficient delivery of traffic to interested edge switches using multicast replication capabilities built into the fabric devices versus burdening the border with extra processing for headend replication. The multicast is encapsulated to interested fabric edge switches, which de-encapsulate the multicast and replicate it to all the interested receivers on the switch. If the receiver is a wireless endpoint, the multicast (just like unicast) is encapsulated by the fabric edge toward the AP associated with the multicast receiver.

**Multicast Forwarding in fabric**

In early versions of SD-Access, IPv4 multicast forwarding within the overlay operates using *headend replication* of multicast packets into the fabric for both wired and wireless endpoints, meaning that border (headend) must take each multicast packet, and for each edge receiver switch, replicate the packet and forward it. Recent versions of SD-Access have the option to use underlay multicast capabilities with many of the platforms, either configured manually or by using LAN automation, for more efficient delivery of traffic to interested edge switches using multicast replication capabilities built into the fabric devices versus burdening the border with extra processing for headend replication. The multicast is encapsulated to interested fabric edge switches, which de-encapsulate the multicast and replicate it to all the interested receivers on the switch. If the receiver is a wireless endpoint, the multicast (just like unicast) is encapsulated by the fabric edge toward the AP associated with the multicast receiver.
The multicast source can exist either within the overlay or outside the fabric. For PIM deployments, the multicast clients in the overlay use a rendezvous point (RP) at the fabric border that is part of the overlay endpoint address space. Cisco DNA Center configures the required multicast protocol support.

<table>
<thead>
<tr>
<th>Tech tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SD-Access solution supports both PIM source-specific multicast and PIM sparse mode (any-source multicast). Overlay IP multicast requires RP provisioning within the fabric overlay, typically using the border. RP redundancy is possible by implementing MSDP between RPs. For multicast optimizations, such as underlay multicast replication, see the release notes for availability using specific platforms.</td>
</tr>
</tbody>
</table>

In addition to communication efficiency, configuring multicast in the underlay network enables overlay networks with a Layer 2 flooding option. The SD-Access Layer-2 flooding option replicates ARP frames, broadcast frames, and link-local multicast frames to all endpoints in an overlay network, using source-specific multicast in the underlay. When enabled, Layer 2 flooding accommodates mDNS and similar services, and addresses connectivity needs for some silent host endpoints requiring receipt of specific non-unicast traffic prior to activating communication.

**Overlay fabric design considerations**

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 used for traffic segmentation inside the overlay. Consider the following in your design 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. Using SGTs also enables scalable deployment of policy without having to do cumbersome updates for policies based on IP addresses, which can be prone to breakage. 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, use an external firewall or other device to enable inter-VN communication. You can choose either or both options to match your requirements.

- **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. Subnets are sized according to the services that they support, versus being constrained by the location of a gateway. Enabling optional broadcast flooding features can limit the subnet size based on the additional bandwidth and endpoint processing requirements for the traffic mix within a specific deployment.

- **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 data plane and control plane**

SD-Access configures the overlay network for fabric data plane encapsulation using the Virtual eXtensible LAN (VXLAN) technology framework. VXLAN encapsulates complete Layer 2 frames for transport across the underlay, with each overlay network identified by a VXLAN network identifier (VNI). The VXLAN header also carries the SGTs required for micro-segmentation.

The function of mapping and resolving endpoint addresses requires a control plane protocol, and SD-Access uses Locator/ID Separation Protocol (LISP) for this task. LISP brings the advantage of routing based not only on the IP address or MAC address as the endpoint identifier (EID) for a device but also on an additional IP address that it provides as a routing locator (RLOC) to
represent the network location of that device. The EID and RLOC combination provides all the necessary information for traffic forwarding, even if an endpoint uses an unchanged IP address when appearing in a different network location. Simultaneously, the decoupling of the endpoint identity from its location allows addresses in the same IP subnetwork to be available behind multiple Layer 3 gateways, versus the one-to-one coupling of IP subnetwork with network gateway in traditional networks.

The following diagram shows an example of two subnets that are part of the overlay network. The subnets stretch across physically separated Layer 3 devices. The RLOC interface is the only routable address that is required to establish connectivity between endpoints of the same or different subnet.

**Figure 5. Example topology—subnet stretching**

For details about the fabric control plane and data plane constructs, as well as a glossary of terms, see the appendices.

**Fabric Data and Control plane design considerations**

When designing the fabric data plane and control plane, there are key requirements to consider: Fabric Control Plane Design, Fabric Border Design and Infrastructure Services.

**Fabric control plane node design considerations**

The fabric control plane contains the database used to identify an 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.

Cisco 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 as a result of each node containing a duplicate copy of control plane
information. The devices supporting the control plane should be chosen to support the HTDB, CPU, and memory needs for an organization based on fabric endpoints.

If the chosen border nodes support the anticipated endpoint scale requirements for a fabric, it is logical to collocate the fabric control plane functionality with the border nodes. However, if the collocated option is not possible (example: Nexus 7700 borders lacking the control plane node function or endpoint scale requirements exceeding the platform capabilities), then you can add devices dedicated to this functionality, such as physical routers or virtual routers at a fabric site. One other consideration for separating Control Plane functionality on to dedicated devices is to support frequent roaming of endpoints across fabric edge nodes. Roaming across fabric edge nodes causes control plane events involving the WLC updating the Control Plane nodes on the mobility of these roaming endpoints. Typically the Core switches in a network form the Border of the SD-Access fabric and adding Control Plane function on these Border nodes in a high-frequency roam environment is not advisable as it impacts the core and the border functionality of the fabric network.

An SD-Access fabric site can support up to six control plane nodes in a wired-only deployment. Cisco AireOS and Catalyst WLCs can communicate with four control plane nodes in a site. To use four control plane nodes in a site with an SD-Access Wireless deployment, two control plane nodes are dedicated to the Guest (discussed later) and two are dedicated to local site traffic. If dedicated Guest Border/Control Plane nodes feature is not used, WLCs can only communicate with two control plane nodes per fabric site.

**Fabric border node design considerations**

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 the End-to-End Virtualization Considerations section.

Larger distributed campus deployments with local site services are possible when interconnected with a transit control plane. You can search for guidance for this topic after these new roles are a generally available feature.

**Infrastructure services design considerations**

SD-Access does not require any changes to existing infrastructure services, although fabric border devices have implemented capabilities to handle the DHCP relay functionality differences assisting fabric deployments. In a typical DHCP relay design, the unique gateway IP address determines the subnet address assignment for an endpoint, in addition to the location to which 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.

**Figure 6. Fabric DHCP packet flow**

![Fabric DHCP packet flow diagram]

To identify the specific DHCP relay source, Cisco DNA Center automates the configuration of the relay agent at the fabric edge with DHCP option 82 including the information option for circuit ID insertion. 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 by the DHCP server itself.

Using a border with advanced DHCP border relay capability allows DHCP server scope configuration to remain unchanged for scopes covering fabric endpoints versus standard non-fabric scope creation. When you are using border nodes with this additional DHCP capability, the borders inspect the DHCP offers returning from the DHCP server (DHCP servers that do not echo this option back must not be used). The offers include the RLOC from fabric edge switch source of the original DHCP request, preserved and returned in the offer. The border node receiving the DHCP offer references the embedded circuit ID with the RLOC information and directs the DHCP offers back to the correct relay destination.

**Wireless capabilities**

SD-Access supports two options for integrating wireless access into the network. One option is to use traditional Cisco Unified Wireless Network 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, which can be useful during migrations to transport CAPWAP-tunneled endpoint traffic from the APs to the WLCs. The other option is fully integrated SD-Access Wireless, extending the SD-Access benefits to include wireless users, where endpoint traffic participates in the fabric directly at the fabric edge switch.

You gain advantages by integrating wireless natively into SD-Access using two additional components: fabric wireless controllers and fabric mode APs. Supported Cisco wireless LAN controllers (WLCs) are configured as fabric wireless controllers to communicate with the fabric control plane, registering Layer 2 client MAC addresses, SGT, and Layer 2 VNI information. The fabric mode APs are Cisco WiFi6 and 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.

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 client traffic carried from wireless endpoints on fabric SSIDs avoids Control and Provisioning of Wireless Access Points (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 forwarding takes the optimum path through the SD-Access fabric to the destination with consistent policy, regardless of wired or wireless endpoint connectivity.

The control plane communication for the APs uses a CAPWAP tunnel to the WLC, which is similar to the traditional Cisco Unified Wireless Network control plane. However, the WLC integration with the SD-Access control plane supports wireless clients roaming to APs across the fabric. The SD-Access fabric 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. APs can be connected directly to edge node switches or can be connected to extended node switches. APs tunnel wireless data traffic using VXLAN encapsulation and rely on the fabric edge node 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 across the wired and wireless domains. Wireless integration also enables the WLC to shed data plane forwarding duties while continuing to function as the centralized services and control plane for the wireless domain.
**Guest wireless services**

If you are not deploying Cisco Unified Wireless Network wireless over the top and require fabric wireless guest access services to the Internet, separate the wireless guests from other network services by creating a dedicated virtual network supporting the guest SSID. Extend the separation of the guest traffic between the fabric border and DMZ, using VRF Lite or similar techniques.

Guest as a VN – Guest traffic can be terminated in its own VN and that VN can be extended to DMZ via traditional methods from the Border. This type of deployment does not require any Guest Anchor to be deployed in the data center.

Using Guest Border/Control Plane – is another way Guest Access can be deployed in a SD-Access fabric network. The Guest traffic is encapsulated right from the fabric edge node to the Guest Border/Control Plane node in the DMZ providing total isolation from other enterprise data traffic.

Support for the workflow needed for the legacy Guest Anchor solution is targeted for a future release in Cisco DNA Center.

Cisco DNA Center automates and manages the workflow for implementing the wireless guest solution for fabric devices only, and wired guest services are not included in the solution.

**Fabric wireless integration Design Considerations**

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 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, WLCs typically connect to a shared services distribution block that is part of the underlay. The preferred distribution block has chassis redundancy as well as the capability to support Layer 2 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.

APs connect into a pre-defined VRF, named INFRA_VRF, which is the same VRF that extended node infrastructure devices use to connect. The VRF has connectivity into the global routing table, and communication from connected devices follows the underlay network to the borders, where reachability to these devices must be advertised externally. This design allows the WLC connection into the network to remain unchanged, while still being able to manage APs at the edge of a fabric domain.
Wireless ‘over the top’ centralized wireless option design considerations

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

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 adjacent to 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, keeping in mind that the benefits of fabric and SD-Access are not extended to and integrated with the wireless when the fabric is used only as an over-the-top transport.

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

Mixed SD-Access Wireless and centralized wireless option design considerations

Many organizations may deploy SD-Access with centralized wireless over-the-top as a first transition step before integrating SD-Access Wireless into the fabric. For this case, an organization should dedicate a WLC for enabling SD-Access Wireless. A WLC dedicated to SD-Access allows use of the same SSID in both the fabric and non-fabric domains, without modifying the existing centralized deployment with changes such as new software versions and AP group configurations.

Organizations can deploy both centralized and SD-Access Wireless services as a migration stage. If there isn’t a requirement to keep the currently deployed centralized wireless software and configuration unchanged, Cisco DNA Center can automate a new
installation supporting both services on the same WLC. In this case, the new installation from Cisco DNA Center does not take into consideration existing running configurations. Instead, Cisco DNA Center automates the creation of the new replacement services.

**Security policy design considerations**

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 when 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. An identity-based approach is also possible in which the network security policies can be deployed depending on 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. Event logs, ACL hit counters, and similar standard accounting tools are available to enhance visibility.

- **Endpoint security:** Endpoints can be infected with malware, compromising data and creating 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 using VNs can control access to applications, such as separating employee transactions from IoT traffic; encryption of the data path in the switching environment using IEEE 802.1AE MACsec 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 virtual network allows for simplified hierarchical network policies. Network-level policy scopes of isolated control and data planes are possible using virtual networks, 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 many 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 the fabric on a device with Cisco TrustSec capability—Inline devices with Cisco TrustSec capability carry the SGT information in a CMD header on the Layer 2 frame. This is the recommended mode of transport outside the SD-Access network.

- Outside the fabric over devices without Cisco 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 https://cisco.com/go/trustsec

Solution management

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, Cisco 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-degree views, as listed in the Solution Components section.

Cisco DNA Center is a required foundational component of SD-Access, enabling automation of device deployments into the network to provide the speed and consistency required for operational efficiency. Organizations then benefit from lower costs 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 Cisco DNA Center 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.

Cisco SD-Access Site Reference Models

Designing for a Cisco SD-Access fabric is flexible to fit many environments, which means it is not a one-design-fits-all proposition. The scale of a fabric can be as small as a single switch or switch stack or as big as one or more three-tier campus deployments. SD-Access topologies should follow the same design principles and best practices associated with a hierarchical design by splitting the network into modular groups, as described in the Campus LAN and Wireless LAN Design Guide.

You create design elements that can be replicated throughout the network by using modular designs. In general, SD-Access topologies should be deployed as spoke networks with the fabric border node at the exit point hub for the spokes. As networks get larger, more varied physical topologies are used to accommodate requirements for specialized network services deployment.

Design strategy for sites reference models

A practical goal for SD-Access designs is to maximize the size of fabric sites within the limits of Cisco DNA Center and within the parameters required for high availability at a site, while minimizing the total number of sites. Use elements from the previous Solution Components section to create the sites.
When designing a network for SD-Access, beyond the business needs and drivers several technical factors must be considered, and the results of these considerations craft the framework of topology and equipment used in the network. These factors are not single-dimensional. These are multi-dimensional items that must be looked at in concert and not strict isolation.

- Greenfield or Brownfield
- Number of Users
- Geography
- Services Location
- Transit Types
- Fusion Routers
- Unified Policy
- Site Survivability
- High Availability
Greenfield and Brownfield

Greenfield or brownfield must be considered, as the goal of a brownfield environment will be to use it in the SD-Access network. Migration is beyond the scope of this document although is accomplished through one of the following approaches:

- **Border Automation - Layer-2 Handoff** – This feature of SD-Access connects a traditional network with an SD-Access network effectively adding the host behind the legacy network to the SD-Access fabric. This is design is a temporary use case while the second approach is taken.

- **Building by building or floor by floor** – Areas of the existing network are converted to SD-Access. This is commonly done closet by closet, floor by floor, or building by building. Migration is done, at minimum, one switch at a time. One VLAN at a time is not supported, as the VLAN may span multiple traditional switches.

Number of Users

The largest driving factor in the equipment and topology for a site other than existing wiring is total number of wired and wireless clients across the location. This will determine the number of physical switch ports and access points required, which may ultimately result in the need for three-tiered or two-tiered network designs. The number of clients may be small enough that the network may be composed of a switch stack.

Geography

Physical Geography impacts the network design. It does not have direct impact on the topology within the site itself, but geography must be considered as it relates to transit types, services locations, survivability and high availability.

Locations that are located within the same metro area (MAN) or campus with multiple buildings in close, physical proximity with interconnect direct fiber can benefit from designing a network for SD-Access for Distributed Campus. This, by extension, allows for native unified policy across the locations along with the potential to have a single services block location.

Locations connected across the WAN or Internet must also considered services and policy as well as the routing infrastructure outside of the fabric overlay used to connect them.

Shared Services

Services such as DHCP, DNS, ISE, and the WLCs are required elements for clients in an SD-Access network. Services are commonly deployed in one of three ways.

In SD-Access for Distributed Campus and in locations distributed across the WAN, services are often deployed at on-premise data centers. These data centers are commonly connected to the core or distribution layers of a centralized location (referred to as Headquarters – HQ – in this document). Traffic is sent from the remote and branch sites back to the Headquarters, and then directed towards the necessary services.

Services may be local to the location. For survivability purposes, a services block may be established at each fabric-site location. Local services ensure that these critical services are not sent across the WAN/MAN and ensure the endpoints are able to access them, even in the event of congestion or down links in the WAN. However, this will also require the need for a fusion router per location to provide access to the shared services.
Transit Types
Transits are simply the physical connections between fabric sites. This connectivity may be MAN, WAN, or Internet. The WAN could be MPLS, IWAN, or other WAN variations. Within Cisco DNA Center, the transits are referred to as SD-Access, IP-Based, or SD-WAN transits.

SD-Access Transits are used in SD-Access for Distributed Campus. Using the SD-Access transit, packets are encapsulated between sites using the fabric VXLAN encapsulation which carries the macro and micro policy constructs.

In IP-Based transits, packets are de-encapsulated from the fabric VXLAN into native IP. Once in native IP, they are forwarded using traditional routing and switching modalities. In Cisco DNA Center, IP-based transits are provisioned with VRF-lite to connect to the upstream device. IP-Based transits are used in two ways: connecting to shared services via fusion routers and connecting to upstream routing infrastructure for connectivity to WAN and Internet.

While the VRF-lite configuration has the same format in both these use-cases, the upstream device is different and referred to by a different name. When the device connects the Fabric border node to shared services, it is called a fusion router. When the upstream device provides connectivity to the WAN or Internet, it is simply called a router or referred to as the routing infrastructure.

SD-WAN transits connect fabric sites through an SD-WAN (Viptela) enabled router. Designing for SD-WAN transits is beyond the scope of this document, as the solution is still evolving.

Fusion Routers
The generic term fusion router comes from MPLS Layer-3 VPN. The basic concept is that the fusion router is aware of the prefixes available inside each VPN (VRF), either because of static routing configuration or through route peering, and can therefore fuse these routes together. A generic fusion router’s responsibilities are to route traffic between separate VRFs (VRF leaking) or to route traffic to and from a VRF to a shared pool of resources in such as DHCP and DNS servers in the global routing table (route leaking). Both responsibilities involve moving routes from one routing table into a separate VRF routing table.

In an SD-Access deployment, the fusion router has a single responsibility: to provide access to shared services for the endpoints in the fabric. There are two primary ways to accomplish this task depending on how the shared services are deployed. The first option is used when the shared services routes are in the GRT. On the fusion router, IP prefix lists are used to match the shared services routes, route-maps reference the IP prefix lists, and the VRF configurations reference the route-maps to ensure only the specifically matched routes are leaked. The second option is to place shared services in a dedicated VRF on the fusion router. With shared services in a VRF and the fabric endpoints in other VRFs, route-targets are used leak between them.

A fusion router can be either a true routing platform, a Layer-3 switching platform, or a firewall that must meet several technological requirements. It must support:

- Multiple VRFs
- 802.1q tagging (VLAN tagging)
- Subinterfaces (when using a router or firewall) or switched virtual interfaces (SVI) (when using a Layer-3 switch)
- BGPv4 and specifically the MP-BGP extensions (RFC 4760 and RFC 7606) for extended communities attributes

WAN and Internet Connectivity
External Internet and WAN connectivity for a fabric site has a significant number of possible variations, and these variations are based on underlying network design. The common similarity among these variations is that the border node is generally connected to a next-hop device that will be traversed to access the Internet and WAN due to its routing information. This
routing infrastructure could be an actual Internet edge router, WAN edge router, an ISP router, or even be the fusion router operating with multiple functions.

The key design consideration is to ensure this routing infrastructure has the physical connectivity and throughput necessary to connect the fabric site to the external world.

**Unified Policy**

Unified policy was a primary driver behind the creation of the SD-Access solution. With unified policy, wired and wireless traffic are both enforced at the access layer (fabric edge node) and users, devices, and applications have the same policy wherever they are connected in the network.

Within a fabric site, the unified policy is enabled and carried through the Segment ID (Group Policy ID) and Virtual Network Identifier fields of the VXLAN-GPO header. Additional details on this header can be found in Appendix A. This allows for both VRF (macro) and SGT (micro) segmentation information to be carried within the fabric site.

In SD-Access for Distributed Campus, the VXLAN-GPO encapsulation format is used to carry data packets between sites. These unified policy constructs are therefore present in every data packet traversing the fabric site or the larger fabric domain.

When designing for a fabric site that has an IP-based transit, considerations must be taken if Unified Policy is desired between the disparate locations. Using an IP-based transit, the fabric packet is de-encapsulated into native IP. This results in loss of policy constructs.

**End to End Macro Segmentation**

SD-Access uses VRFs (Virtual Networks or VNs) for macro segmentation. VRFs maintain a separate routing and switching instance for the devices, interfaces, and subnets within it. Within the fabric site, Cisco DNA Center provisions the configuration for the user-defined VRFs.

Segmentation beyond the fabric site has multiple variations depending on the type of Transit. In SD-Access for Distributed Campus and SD-WAN transits, the VN information is natively carried within the packet.

In IP-based transit, due to the de-encapsulation, that policy information can be lost. Two approaches exist to carry VN information between fabric sites using an IP-based transit. The most straightforward approach, although the least deployed due to SP equipment being beyond the engineer’s administrative control, is to configure VRF-lite hop-by-hop between each fabric site.

A second design option uses VPNv4 addresses family in multi-protocol BGP to carry the macro segmentation information. Because BGP is a point-to-point TCP session between peers, the policy constructs can traverse the service provider WAN network using it simply as an IP forwarding path between BGP routing infrastructure at each fabric site.

**End to End Micro Segmentation**

SD-Access uses SGTs (Scalable group tags) for micro segmentation. SGTs use metadata in the form of unique tag to assign host to groups and apply policy based on those groups. Within the fabric overlay, edge nodes and border nodes use SGACLs downloaded from ISE to make enforcement decisions based on these SGTs.

Segmentation beyond the fabric site has multiple variations depending on the type of Transit. In SD-Access for Distributed Campus and SD-WAN transits, the VN information is natively carried within the packet.

In IP-based transit, due to the de-encapsulation, that policy information can be lost. Two approaches exist to carry SGT information between fabric sites using an IP-based transit. The most straightforward approach, although the least deployed due
to SP equipment being beyond the engineer’s administrative control, is to configure inline tagging (CMD) hop-by-hop between each fabric site. A second design option is to use SXP to carry the IP-to-SGT bindings between sites. Using SXP, these bindings can be carried over GRE, IPsec, DMVPN, and GETVPN circuits between sites.

SXP has both scaling and enforcement point implications that must be considered. Between fabric sites, SXP can be used to enforce the SGTs at either the border nodes or at the routing infrastructure north bound of the border. If enforcement is done at the routing infrastructure, CMD is used to carry the SGT information inline from the border node. For additional details on deployment scenarios, SGTs over GRE and VPN circuits, and scale information, please see SD-Access Segmentation Design Guide.

Site Survivability

In the event that the WAN and MAN connections are unavailable, any services access across these circuits are unavailable to the endpoints in the fabric. The need for site survivability is determined by balancing the associated costs of the additional equipment and the business drivers behind the deployment while also factoring in the number of impacted users at the site.

Designing an SD-Access network for site survivability involves having shared services local to the site. When shared services are site-local, a fusion router is necessary to access these services.

High Availability

High availability can go hand in hand with Site Survivability. A site with single fabric border, control plane node, or wireless controller risk single points of failure in the event of a device outage. When designing for High Availability in an SD-Access network, it is important to note that redundant devices do not increase the overall scale. Redundant Fabric border nodes and fabric control plane nodes operate in an active-active fashion and WLCs operate as active-standby pairs.

Fabric Site Reference Models

To better understand common site designs, simple reference categories are used. The numbers are used as guidelines only and do not necessarily match any specific limits for devices within a design.

- **Very small site**—Uses Fabric in a Box to cover a single wiring closet, with resilience supported by switch stacking; designed for less than 2,000 endpoints, less than 8 VNs, and less than 100 APs; the border, control plane, edge, and wireless functions collocated on a single redundant platform.

- **Small site**—Covers a single office or building; designed to support less than 10,000 endpoints, less than 32 VNs, and less than 200 APs; the border is collocated with the control plane function on one or two devices and a separate wireless controller has an optional HA configuration.

- **Medium site**—Covers a building with multiple wiring closets or multiple buildings; designed to support less than 25,000 endpoints, less than 64 VNs, and less than 1,000 APs; the border is distributed from or collocated with the control plane function using redundant, dedicated, non-stacking devices, and a separate wireless controller has an HA configuration.

- **Large site**—Covers a large building with multiple wiring closets or multiple buildings; designed to support less than 50,000 endpoints, less than 64 VNs, and less than 2,000 APs; multiple border exits are distributed from or collocated with the control plane function on redundant devices with dedicated non-stacking edge devices, and a separate wireless controller has an HA configuration.

Each fabric site includes a supporting set of control plane nodes, edge nodes, border nodes, and wireless LAN controllers, sized appropriately from the listed categories. ISE policy nodes are also distributed across the sites to meet survivability requirements. In a single physical network, multiple fabrics can be deployed. For this case, individual fabric elements (control plane nodes, border nodes, edge nodes, and WLCs) are assigned to a single fabric only.
Each reference model takes the multidimensional design considerations along with endpoint count to provide guidelines to stay within for similar site design sizes. These do not necessarily match specific limits for devices used in a design of this site size.
**Very Small Site Design — Reference Model**

The Very Small Site Reference model covers a single wiring closet and typically less than 2,000 endpoints. The central component of this design is a switch stack operating in all three fabric roles of control plane node, border node, and edge node. When a switch is deployed in this way, it is referred to as *Fabric-in-a-Box*.

**Figure 9. Physical Topology — Very Small Site Design**

**Very Small Site Considerations**

Due to the smaller number of endpoints, high availability and site survivability are not common requirements for a very small site design. Common to all reference designs, site-local services of DHCP, DNS, WLCs, and ISE provide resiliency and survivability at although at the expense of increased complexity and equipment including a fusion router.

If shared services are deployed locally, the fusion router is commonly a switch directly connected to the Fabric-in-a-Box with services deployed as virtual machines on UCS C-Series connected to the fusion. An alternative is to deploy a UCS E-series blade servers in either the WAN routing infrastructure or fabric routers to virtualize the shared services.

High availability in this design is provided through *Stackwise-480* which combines multiple physical switches into a single logical switch and *StackPower* to provide power redundancy between members in the switch stack. If a chassis switch is used, high availability is provided through redundant supervisors and redundant power supplies.

Wireless LAN controllers can be deployed as physical units directly connected to the Fabric-in-a-Box or deployed as the embedded Catalyst 9800 controller. When using the embedded Catalyst 9800 with a switch stack or redundant supervisor, AP and Client SSO are provided automatically.

When using a switch stack, links to the upstream routing infrastructure should be used from different stack members. With chassis switches, links should be connected through different supervisors. To prepare for border node handoff automation
along with have initial IP reachability, SVIs and trunk links are commonly deployed between the small site switches and the upstream routing infrastructure.

The Catalyst 9300 Series in a stack configuration with the embedded Catalyst 9800 Series wireless LAN controller capabilities is an optimal platform in this design. Other available platforms such as the Catalyst 9500 Series add additional physical connectivity options, but without the added resiliency using StackWise-480 and StackPower.

Table 1. Very Small Site Reference Model Design – Guidelines

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints, target fewer than</td>
<td>2,000</td>
</tr>
<tr>
<td>Fabric nodes, maximum</td>
<td>1</td>
</tr>
<tr>
<td>Control plane nodes, collocated</td>
<td>1</td>
</tr>
<tr>
<td>Border nodes, collocated</td>
<td>1</td>
</tr>
<tr>
<td>Virtual networks, target fewer than</td>
<td>8</td>
</tr>
<tr>
<td>IP pools, target fewer than</td>
<td>8</td>
</tr>
<tr>
<td>Access points, target fewer than</td>
<td>100</td>
</tr>
</tbody>
</table>
Small Site Design - Reference Model

The Small Site Reference model covers a building with multiple wiring closets or multiple buildings and typically has less than 10,000 endpoints. The physical network is usually a 2-Tier collapsed core/distribution and access layer.

Figure 10. Physical Topology — Small Site Design

Small Site Considerations

In a small site, high availability is provided in the fabric nodes by collocating the border node and control plane node functionality on the collapsed core switches. For both resiliency and alternative forwarding paths in the overlay and underlay, the collapsed core switches should be directly connected to each other with a crosslink.

Due to the number of endpoints, small sites generally do not use SD-Access Embedded Wireless. Provided there are less than 200 APs and 4000 clients, embedded wireless can be deployed along with the collocated border node and control plane node functions on the collapsed core switches.

To support a larger number of clients or access points, physical WLC are deployed. To enable high availability either in the device using an HA-SSO pair or through physical connectivity, a services block is deployed. The WLCs are connected to the services block switch through layer-2 port-channels to provide redundant interfaces. The services block is commonly a small switch stack that is connected to both collapsed core switches. This services block can be used as a fusion router if DHCP and DNS servers are site-local.

Table 2. Small Site Reference Design – Guidelines

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints, target fewer than</td>
<td>10,000</td>
</tr>
<tr>
<td>Fabric nodes, maximum</td>
<td>25</td>
</tr>
<tr>
<td>Control plane nodes</td>
<td>2</td>
</tr>
</tbody>
</table>
### Medium Site Design – Reference Model

The Medium Site Reference Model covers a building with multiple wiring closets or multiple buildings and is designed to support less than 25,000 endpoints. The physical network is usually a 3-tier network with core, distribution, and access. It may even contain a router super-core that aggregates multiple buildings and serves as the network egress point to the WAN and Internet.

### Medium Site Considerations

In a medium site, high availability is provided in the fabric nodes by dedicating devices as border nodes and control plane nodes rather than collocating the functions on a device. For both resiliency and alternative forwarding paths in the overlay and underlay, the collapsed core switches should be directly connected to each other with a crosslink. Dedicated control plane nodes are generally connected to the core switches at the site. For optimal forwarding and redundancy, they should have connectivity through both cores.

Medium sites cannot take advantage of SD-Access Embedded Wireless due to the number of endpoints and the distributed control plane nodes and border nodes and therefore physical WLC are deployed. To enable high availability an HA-SSO pair is deployed with redundant physical connectivity to a services block using layer-2 port-channels. The WLC should be connected to each other through their RP port. The services block is commonly fixed configuration switches operating in VSS or Stackwise.
Virtual that are connected to both core switches. This services block switches can be used as a fusion router if DHCP and DNS servers are site-local.

Table 3. Medium Site Reference Design – Guidelines

<table>
<thead>
<tr>
<th>Category</th>
<th>Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints, target fewer than</td>
<td>25,000</td>
</tr>
<tr>
<td>Fabric nodes, maximum</td>
<td>25</td>
</tr>
<tr>
<td>Control plane nodes</td>
<td>2-4</td>
</tr>
<tr>
<td>(limit to 2 + 2 guest for SD-Access Wireless)</td>
<td></td>
</tr>
<tr>
<td>Border nodes</td>
<td>2</td>
</tr>
<tr>
<td>Virtual networks, target fewer than</td>
<td>64</td>
</tr>
<tr>
<td>IP pools, target fewer than</td>
<td>300</td>
</tr>
<tr>
<td>Access points, target fewer than</td>
<td>1,000</td>
</tr>
</tbody>
</table>
Large Site Design – Reference Model

The Large Site Reference Model covers a building with multiple wiring closets or multiple buildings. The physical network is usually a 3-tier network with core, distribution, and access, and is designed to support less than 50,000 endpoints. This network is large enough to require dedicated services exit points such as a dedicated data center, shared services block, and Internet services.

Figure 12. Physical Topology – Large Site Design

Large Site Considerations

The Large Site is commonly the Headquarters location in a multiple-fabric deployment. The Enterprise Edge Firewall (Perimeter Firewall) is generally deployed at this location, and internet traffic from remote sites are tunnel back to this site to be processed through it before being place on the Internet. Cisco DNA Center and the primary ISE PAN are generally deployed at this location.

Control plane nodes and border nodes should be dedicated devices deployed as redundant pairs. Dedicated control plane nodes should be connected to each core switch to provide for resiliency and redundant forwarding paths.

A Wireless LAN controller HA-SSO pair is deployed with redundant physical connectivity to a services block using layer-2 port-channels. The WLC should be connected to each other through their RP port. The services block is commonly part of the on-premise data center network. This services block may be multiple hops downstream in the data center, although the DC-core is connected to either the core or the distribution switches to provide reachability. With multiple devices between the services
block and core switches, the fusion router services device location may vary. Cisco Nexus data center switches with appropriate license level and capabilities can be used for this function.

Dedicated internal border nodes are commonly used to connect the site to the data center core while dedicated external border nodes are used to connect the site to the MAN, WAN, and Internet. Dedicated redundant routing infrastructure and firewalls are used to connect this site to external resources, and border nodes should be fully meshed to these and to each other. Although the topology depicts the border at a campus core, the border at a Large Site is often configured separately from the core switches at another aggregation point.

The Large site may contain dedicated Guest fabric border and control plane nodes. These devices are generally deployed with the fabric roles collocated rather than distributed and are physically accessed and connected to the DMZ. This provides complete control plane and data plane separate between Guest and Enterprise traffic and optimizes Guest traffic to be sent directly to the DMZ without the need for an Anchor WLC.

Table 4. Large Site Reference Design – Guidelines

<table>
<thead>
<tr>
<th>Endpoint, target fewer than</th>
<th>50,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric nodes, maximum</td>
<td>1,000</td>
</tr>
<tr>
<td>Control plane nodes</td>
<td>2-6</td>
</tr>
<tr>
<td>(limit to 2 + 2 guest for SD-Access Wireless)</td>
<td></td>
</tr>
<tr>
<td>Border nodes</td>
<td>2-4</td>
</tr>
<tr>
<td>Virtual networks, target fewer than</td>
<td>64</td>
</tr>
<tr>
<td>IP pools, target fewer than</td>
<td>500</td>
</tr>
<tr>
<td>Access points, target fewer than</td>
<td>2,000</td>
</tr>
</tbody>
</table>
SD-Access for Distributed Campus Design – Reference Model

SD-Access for Distributed Campus is a metro-area solution that connects multiple, independent fabric sites together while maintaining the security policy constructs (VRFs and SGTs) across these sites. While multi-site environments and deployments have been supported with SD-Access for some time, there has not been an automated and simplistic way to maintain policy between sites. At each site’s fabric border node, fabric packets were de-encapsulated into native IP. Combined with SXP, policy could be carried between sites using native encapsulation. However, this policy configuration was manual, mandated use of SXP to extend policy between sites, and involved complex mappings of IP to SGT bindings within the Identity Services Engine.

With SD-Access for Distributed Campus, SXP is not required, the configurations are automated, and the complex mappings are simplified. This solution enables inter-site communication using consistent, end-to-end automation and policy across the metro network.

Software-Defined Access for Distributed Campus uses control plane signaling from the LISP protocol and keeps packets in the fabric VXLAN encapsulation between fabric sites. This maintains the macro- and micro-segmentation policy constructs of VRFs and SGT, respectively, between fabric sites. The original Ethernet header of the packet is preserved to enable the Layer-2 overlay service of SD-Access Wireless. The result is a network that is address-agnostic because policy is maintained through group membership.

Figure 13. Physical Topology – SD-Access for Distributed Campus

Distributed Campus Considerations
The core components enabling the Distributed Campus solution are the SD-Access transit and the transit control plane nodes. Both are new architectural constructs introduced with this solution. The SD-Access transit is simply the physical metro-area connection between fabric sites in the same city, metropolitan area, or between buildings in a large enterprise campus.

**SD-Access Transit**

SD-Access Transits are used in SD-Access for Distributed Campus. The key consideration for the Distributed Campus design using SD-Access transit is that the network between fabric sites and to Cisco DNA Center should be created with campus-like connectivity. The connections should be high-bandwidth (Ethernet full port speed with no sub-rate services), low latency (less than 10ms as a general guideline), and should accommodate the MTU setting used for SD-Access in the campus network (typically 9100 bytes). The physical connectivity can be direct fiber connections, leased dark fiber, Ethernet over wavelengths on a WDM system, or metro Ethernet systems (VPLS, etc.) supporting similar bandwidth, port rate, delay, and MTU connectivity capabilities. Using the SD-Access transit, packets are encapsulated between sites using the fabric VXLAN encapsulation.

**Transit Control Plane Nodes**

The transit control plane nodes track all aggregate routes for the fabric domain and associate these routes to fabric sites. When traffic from an endpoint in one site needs to send traffic to an endpoint in another site, the transit control plane node is queried to determine to which site's border node this traffic should be sent. The role of transit control plane nodes is to learn which prefixes are associated with each fabric site and to direct traffic to these sites across the SD-Access transit using control-plane signaling.

**Transit Control Plane Deployment Location**

The transit control plane nodes do not have to be physically deployed in the Transit Area (the metro connection between sites) nor do they need to be dedicated to their own fabric site, although common topology documentation often represents them in this way. These devices are generally deployed in their own dedicated location, only accessible through the SD-Access transit metro network, although this is not a requirement.

While accessible only via the Transit Area, these routers do not act as a physical-transit hop in the data packet forwarding path. Rather, they function similarly to a DNS server in that they are queried for information, even though data packets do not transit through them. This is an important consideration.

**Key Considerations**

The transit between sites is best represented and most commonly deployed as direct or leased fiber over a Metro Ethernet system. While Metro-E has several different varieties (VPLS, VPWS, etc.), the edge routers and switches of each site ultimately exchange underlay routes through an Interior Gateway Routing (IGP) protocol. In SD-Access, this is commonly done using the IS-IS routing protocol, although other IGPs are supported.

IP reachability must exist between fabric sites. Specifically, there must be a known underlay route between the Loopback 0 interfaces on all fabric nodes. Existing BGP configurations and peerings on the transit control plane nodes could have complex interactions with the Cisco DNA Center provisioned configuration and should be avoided. BGP private AS 65540 is reserved for use on the transit control plane nodes and automatically provisioned by Cisco DNA Center. The transit control plane nodes should have IP reachability to the fabric sites through an IGP before being discovered or provisioned.

Traversing the transit control plane nodes in the data forwarding path between sites is not recommended. Transit control plane nodes should always be deployed as a pair of devices to provide resiliency and high availability.

**Platform roles and capabilities considerations**

Choose your SD-Access network platform based on capacity and capabilities required by the network, considering the recommended functional roles. Roles tested during the development of this guide are noted in the related deployment guides at https://www.cisco.com/go/cvd/campus.
Refer to the [SD-Access Hardware and Software Compatibility Matrix](#) for the most up-to-date details about which platforms and software are supported for each version of Cisco SD-Access. Your physical network design requirements drive the platform and software choices. Platform capabilities to consider in an SD-Access deployment:

- A wide range of Cisco Catalyst 9000 Series devices (both wired and wireless) and Catalyst 3850 and 3650 are supported; however, only certain devices are supported as fabric edge, border, and control plane node roles, and the available roles may be expanded as newer versions of Cisco DNA Center and Cisco IOS-XE software are released.

- Additional devices such as the Cisco Catalyst 4500 and 6800 Series and Cisco Nexus 7700 Series are also supported, but there may be specific supervisor module, line card module, and fabric-facing interface requirements. Additionally, the roles may be reduced. For example, Nexus 7700 software may restrict the SD-Access role to being used only as an external border, also requiring a separate control plane node.

- A variety of routing platforms are supported as control plane and border nodes, such as the Cisco ISR 4400 and 4300 Series Integrated Services routers, Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers, but none can be fabric edge nodes. The Cisco Cloud Services Router 1000V Series is also supported, but only as a control plane node.

- The Cisco Catalyst 9800 (standalone and embedded), 8540, 5520, and 3504 Series Wireless LAN Controllers have specific software requirements for their support. Similarly, the Cisco Catalyst 9100 and Cisco Aironet Wave 2 and Wave 1 APs call for specific software versions.

- Cisco ISE must be deployed with a version compatible with Cisco DNA Center.
Migration to SD-Access

You can readily create SD-Access greenfield networks by adding the infrastructure components, interconnecting them, and using Cisco 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 overlays, what is the strategy for integrating those overlays 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 overlays are used to segment and virtualize within the fabric, what requirements exist for extending them beyond the fabric? Is infrastructure in place to support Cisco 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.

To assist with network migration, SD-Access supports a Layer 2 border construct that can be used temporarily during a transition phase. Create a Layer 2 border handoff using a single border node connected to the existing traditional Layer 2 access network, where existing Layer 2 access VLANs map into the SD-Access overlays. You can create link redundancy between a single Layer 2 border and the existing external Layer 2 access network using EtherChannel. Chassis redundancy on the existing external Layer 2 access network can use StackWise switch stacks, Virtual Switching System, or StackWise Virtual configurations. The number of hosts supported on a Layer 2 border varies depending on SD-Access releases, with the earliest releases limited to 4,000 hosts. Plan for the fabric DHCP services to be supporting both the fabric endpoints and migrating non-fabric Layer 2 network devices at connection time.

For detailed coverage of migration topics, see the Software-Defined Access Migration guide on Cisco.com.
Appendix A—SD-Access Fabric Protocols

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 tag the original Layer 2 frame using UDP/IP over the Layer 3 network. Each overlay network is called a VXLAN segment and is identified using a 24-bit VXLAN network identifier, which supports up to 16 million VXLAN segments.

Figure 14. RFC 7348 VXLAN header

The SD-Access fabric uses the VXLAN data plane to provide transport of the full original Layer 2 frame and additionally uses Locator/ID Separation Protocol as the control plane to resolve endpoint-to-location mappings. The SD-Access fabric replaces 16 of the reserved bits in the VXLAN header to transport up to 64,000 SGTs, using a modified VXLAN-GPO format described in https://tools.ietf.org/html/draft-smith-vxlan-group-policy-05.

The VNI maps to a virtual routing and forwarding 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 or MAC address is used as the endpoint identifier for a device, and an additional IP address is used as an 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 underlay 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. 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 to identify the destination RLOC for traffic encapsulation. As with DNS, a local node probably does not have the information about everything in a network but, instead, asks for the information only when local hosts need it to communicate (pull model), and the information is then cached for efficiency.

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 is 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.
## Appendix B—Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>authentication, authorization, and accounting</td>
</tr>
<tr>
<td>ACL</td>
<td>access control list</td>
</tr>
<tr>
<td>AP</td>
<td>access point</td>
</tr>
<tr>
<td>BGP</td>
<td>border gateway protocol</td>
</tr>
<tr>
<td>CAPWAP</td>
<td>control and provisioning of wireless access points protocol</td>
</tr>
<tr>
<td>Cisco DNA</td>
<td>Cisco Digital Network Architecture</td>
</tr>
<tr>
<td>CMD</td>
<td>Cisco Meta Data</td>
</tr>
<tr>
<td>DMZ</td>
<td>firewall demilitarized zone</td>
</tr>
<tr>
<td>EID</td>
<td>endpoint identifier</td>
</tr>
<tr>
<td>HTDB</td>
<td>host tracking database</td>
</tr>
<tr>
<td>IGP</td>
<td>interior gateway protocol</td>
</tr>
<tr>
<td>ISE</td>
<td>Cisco Identity Services Engine</td>
</tr>
<tr>
<td>LISP</td>
<td>Locator/ID Separation Protocol</td>
</tr>
<tr>
<td>MR</td>
<td>Map-Resolver</td>
</tr>
<tr>
<td>MS</td>
<td>Map-Server</td>
</tr>
<tr>
<td>MTU</td>
<td>maximum transmission unit</td>
</tr>
<tr>
<td>RLOC</td>
<td>routing locator</td>
</tr>
<tr>
<td>SD-Access</td>
<td>Software-Defined Access</td>
</tr>
<tr>
<td>SGACL</td>
<td>scalable group access control list</td>
</tr>
<tr>
<td>SGT</td>
<td>scalable group tag</td>
</tr>
<tr>
<td>SXP</td>
<td>scalable group tag exchange protocol</td>
</tr>
<tr>
<td>VLAN</td>
<td>virtual local area network</td>
</tr>
<tr>
<td>VN</td>
<td>virtual network</td>
</tr>
<tr>
<td>VNI</td>
<td>virtual extensible LAN network identifier</td>
</tr>
<tr>
<td>VRF</td>
<td>virtual routing and forwarding</td>
</tr>
<tr>
<td>VXLAN</td>
<td>virtual extensible LAN</td>
</tr>
</tbody>
</table>
Feedback

For comments and suggestions about this guide and related guides, join the discussion on Cisco Community at https://cs.co/en-cvds.