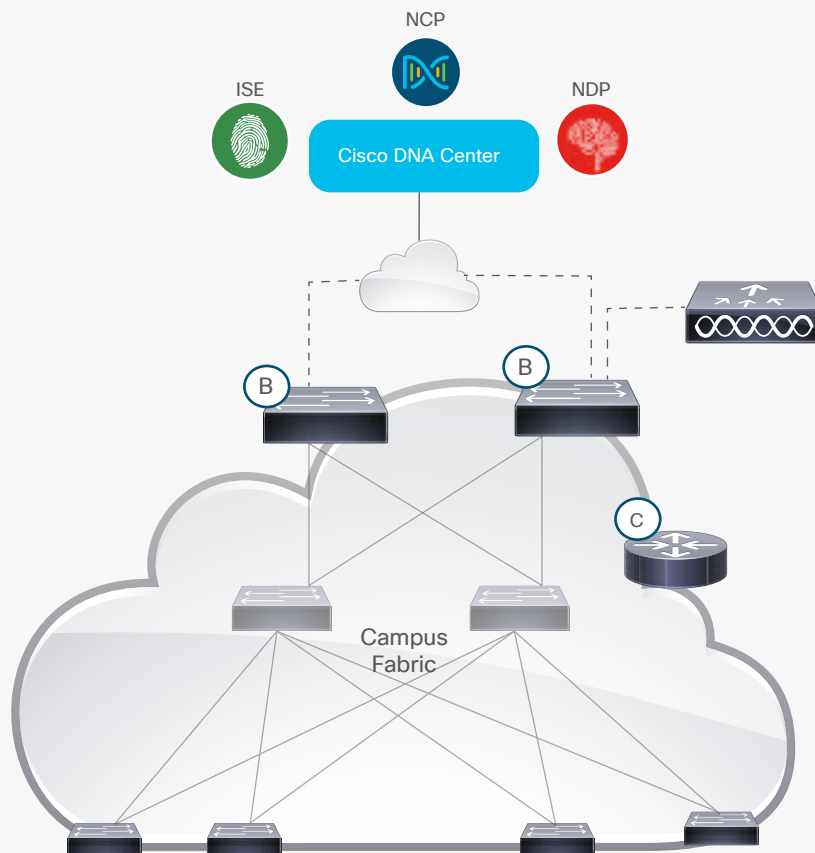ıllıllı
CISCO

Software-Defined Access 1.0

What is Cisco Software-Defined Access?

The Cisco® Software-Defined Access (SD-Access) solution uses **Cisco DNA Center** to provide intent-based **policy, automation,** and **assurance** for your **Campus Fabric** wired and wireless access network.

This paper describes the **Cisco SD-Access 1.0** solution at a medium technical level. It is the counterpart to the Solution Overview paper, which describes the business value of Cisco SD-Access 1.0

It is designed to be the first document a **technical decision maker** will read to begin their journey with SD-Access.

Figure 1. Cisco SD-Access

Contents

Introduction

Note: The Cisco SD-Access 1.0 solution described here includes both the initial 1.0 (Controlled Availability) release, as well as the subsequent 1.1 (General Availability) and 1.2 releases.

This document introduces the five basic layers of the SD-Access 1.0 architecture:

- **Physical layer:** Contains the hardware elements, such as routers, switches and wireless platforms, interfaces and links, and clusters or virtual switches, as well as server appliances.
- **Network layer:** Contains the control plane, data plane, and policy plane elements that make up the network underlay and fabric overlay.
- **Controller layer:** Contains the software system management and orchestration elements and associated subsystems, such as automation, identity, and analytics.
- **Management layer:** Contains the elements that users interact with, in particular the Graphical User Interface (GUI), as well as APIs and Command-Line Interfaces (CLIs) where applicable.
- **Partner ecosystem:** Contains all of the Cisco and third-party partner systems that are capable of augmenting and/or leveraging services within SD-Access.

Each of these layers is described here, with diagrams that describe the layers and how they relate to one another. Where relevant, we provide links to other documents and/or presentations that discuss each aspect in greater detail.

**TIP:** Use the table of contents and/or navigation pane to quickly jump to various sections.

Architecture

Cisco SD-Access is one of the main elements of the **Cisco Digital Network Architecture** (Cisco DNA). Cisco DNA is the blueprint for the future of intent-based networking in Cisco Enterprise Networks. To read more about the overall Cisco DNA solution and its benefits, refer to the following link: www.cisco.com/go/dna.

As the name suggests, the main focus of SD-Access is on enterprise campus and branch "access" network environments (rather than data center, service provider, WAN, etc.), as a part of the overall Cisco DNA solution. To read more about the SD-Access solution and its benefits, refer to the following link: www.cisco.com/go/sda.

As described in the introduction, the Cisco SD-Access 1.0 solution can be divided into five basic layers, and then further divided from there. This section focuses on the relationships between these five basic layers, from an overall architectural perspective. Figure 2 illustrates the layers and their relation to one another.

Figure 2.   Cisco DNA SD-Access architecture
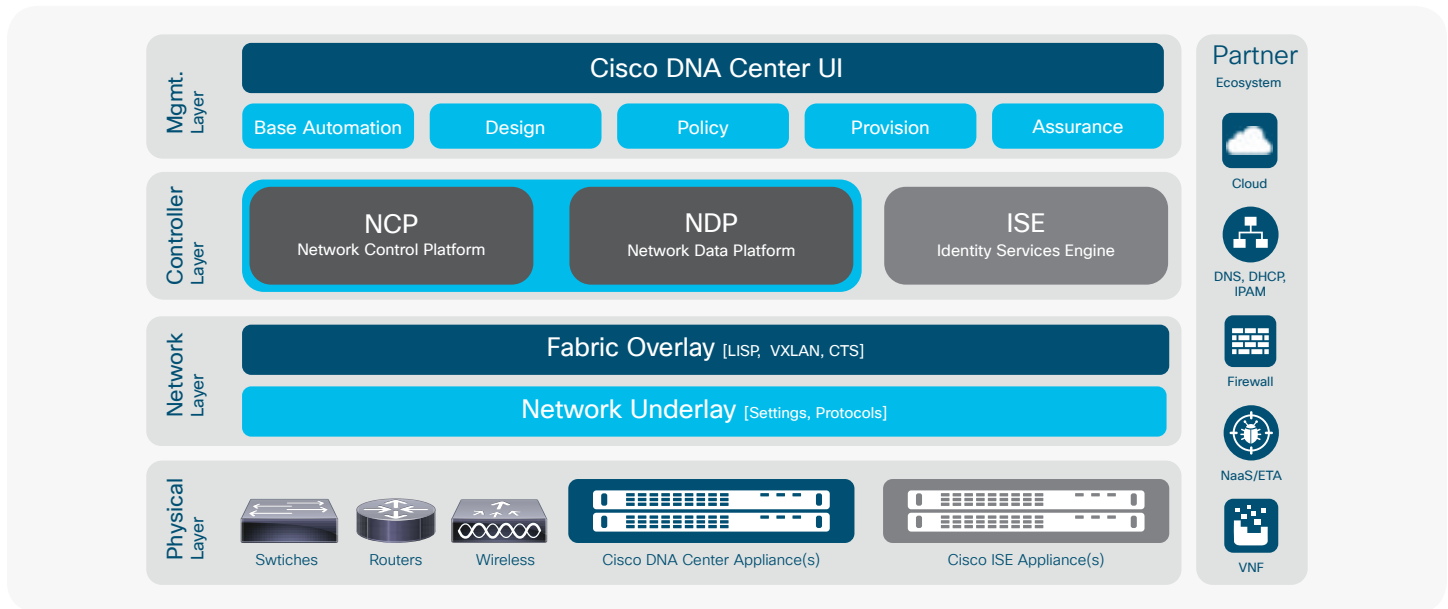
Based on over 30 years of networking experience, Cisco SD-Access uses hardware and software technologies that have been leveraged from existing technologies. Thus, many of the elements may already be familiar to you. The difference is in how these technologies are integrated together to create Cisco SD-Access.

Physical layer overview

At the bottom, we naturally have the **physical layer** (Figure 3).

Figure 3.   The physical layer
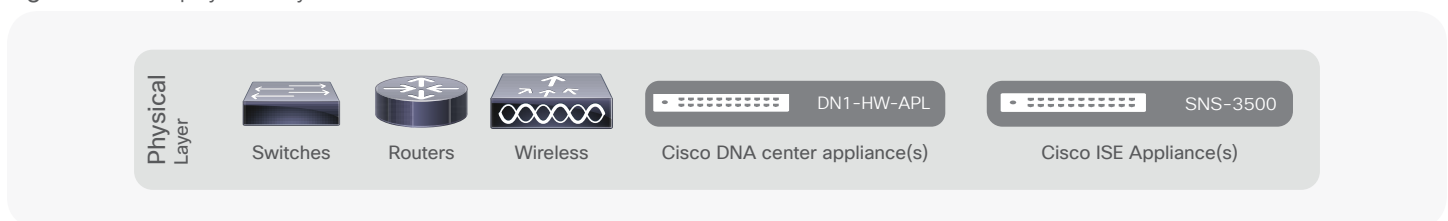
This layer includes enterprise network devices (hardware), the various **router**, **switch**, and **wireless platforms**, their operating systems (software), and the interfaces and links that connect them. It also includes **server appliances** (hardware), their operating systems (software), and the interfaces and links that connect them to network devices.

The important part of this layer (from an architecture perspective) is how the physical hardware and software provide specific capabilities that enable the overall SD-Access solution. For example, all of the supported network devices require the ability to process special frame encapsulations, maintain specific protocols and tables, provide programmable APIs, and offer other capabilities necessary to support the network layer.

For more details, refer to the physical layer section.

Network layer overview

Running on top of the physical layer is the **network layer** (Figure 4).

Figure 4.   The network layer
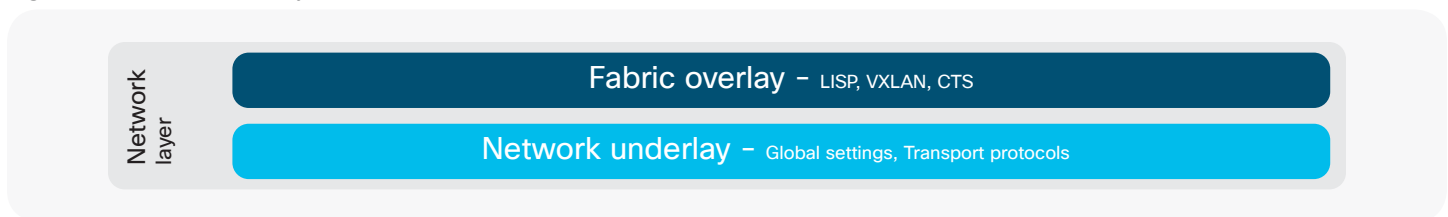
This layer can be further divided into two subcategories:

- **Network underlay:** Contains the settings, protocols, and tables, as well as stacking or device virtualization techniques, for the physical devices that provide a transport layer (under the overlay).
- **Fabric overlay:** Contains the settings, forwarding and policy protocols, and tables for the devices that provide a logical services layer (over the underlay).

The **network underlay** is analogous to your existing Layer 2/Layer 3 network and is most closely associated with the physical layer, but with a simplified focus on transporting data packets between network devices for the (logical) overlay. The **fabric overlay** is a mostly a logical (tunneled) network that virtually interconnects all of the network devices (to form a "fabric") and this abstracts the inherent complexities and limitations of the (physical) underlay.

The important part of this layer (from an architecture perspective) is that the two sublayers form the "access" and "fabric" aspects of the overall SD-Access solution (in a traditional networking sense). These two sublayers work together to deliver the data packets to and from the network devices participating in SD-Access.

For more details, refer to the network layer section.

Controller layer overview

Managing the network layer is the **controller layer** (Figure 5).

Figure 5.   The controller layer
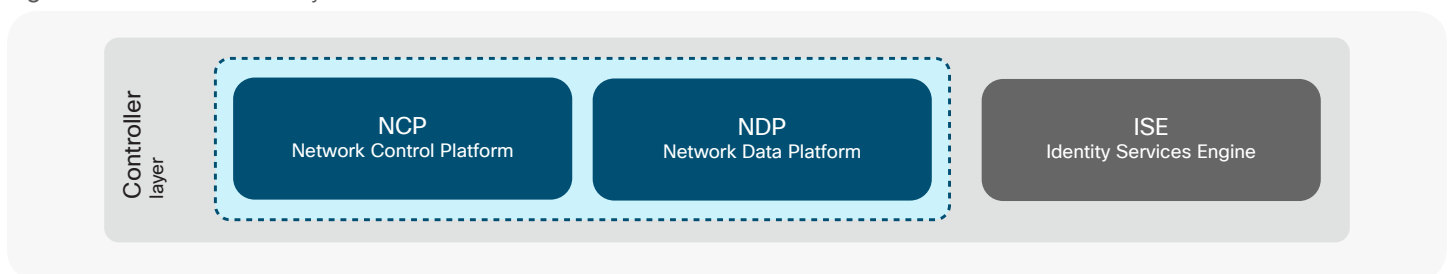
This layer can be further divided into three subsystems:

- **Base and fabric automation:** Contains the application settings, protocols, and tables to support the automation of network devices (underlay and overlay) and related services (Cisco Network Controller Platform [NCP]).
- **Assurance and analytics:** Contains the application settings, protocols, and tables to support the collection and analysis of user, network, and application states (Cisco Network Data Platform [NDP]).
- **Identity and policy services:** Contains the application settings, protocols, and tables to support endpoint identification and policy enforcement services (Cisco Identity Services Engine [ISE]).

Note: Controller services run on the server appliances noted in the physical layer section.

These controller subsystems form an abstraction layer to hide the complexities and dependencies of managing so many network devices and protocols. For example, whenever you add, remove, or update something in the SD-Access fabric, these are the software subsystems responsible for ensuring that it is added, removed, or updated correctly.

All of the "base" and "fabric" automation services are provided by **Cisco NCP**, and all of the "analytics" and "assurance" services are provided by **Cisco NDP**. Both of these subsystems run together on the same physical appliance(s). All of the "identity" and "policy" services are provided by **Cisco ISE**, which runs on one or more separate appliances. These controller subsystems may run on single or multiple appliances in a standalone, redundant, or distributed model, on your premises or (in the future) as cloud-based services.

The important part of this layer (from an architecture perspective) is that these three subsystems form the "software-defined" aspect of the overall SD-Access solution. Each subsystem is responsible for managing a part of the solution, and for exchanging contextual information with the others. These three subsystems work together to deliver a fully automated intent-driven, closed-loop management system for devices participating in Cisco SD-Access.

For more details, refer to the controller layer section.

Management layer overview

Users interact with the controller layer via the **management layer** (Figure 6).

Figure 6.   The management layer
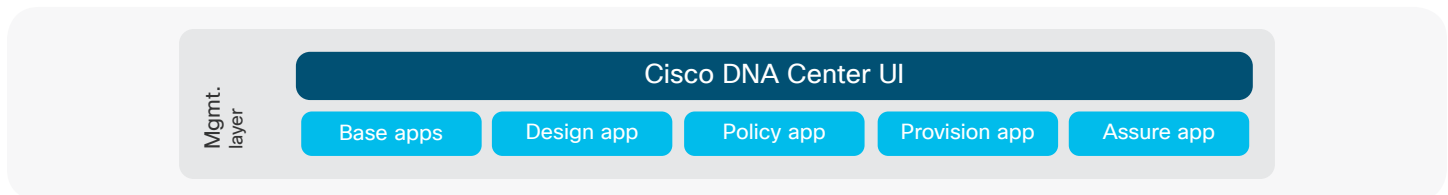
This layer can also be further divided, although in a variable manner, because the various user workflows can either be exposed as separate (smaller) apps or merged together as individual steps within a single (larger) app.

There are two basic app types:

- **Cisco DNA Center settings:** Contain the controller settings, APIs, and tables to support communications between subsystems, as well as for integrating partner services.
- **Cisco DNA Center applications:** Contain the workflow tools and contextual application data to support various user workflows (such as design, policy, provisioning, and assurance).

Cisco DNA Center settings are analogous to settings in other network management systems (for example, they configure role-based access [permissions], redundancy, backups, upgrades, etc.), but they also include specific tools and settings for integration between controller subsystems, as well as APIs to integrate with various external (partner) systems. **Cisco DNA Center applications** are designed for simplicity and are based on the primary user workflows defined by Cisco DNA: design, policy, provisioning, and assurance.

The important part of this layer (from an architecture perspective) is that these two app types are how the user interacts with the SD-Access solution, how Cisco DNA Center interacts with partner systems, and how it provides the "intent-based" aspect of Cisco DNA. This is a flexible and customizable user interface and user experience (UI/UX) system that will allow the solution to evolve in the future.

For more details, refer to the management layer section.

Partner layer overview

Through the power of APIs, we are building a **partner ecosystem** (Figure 7).

Figure 7.   The partner layer
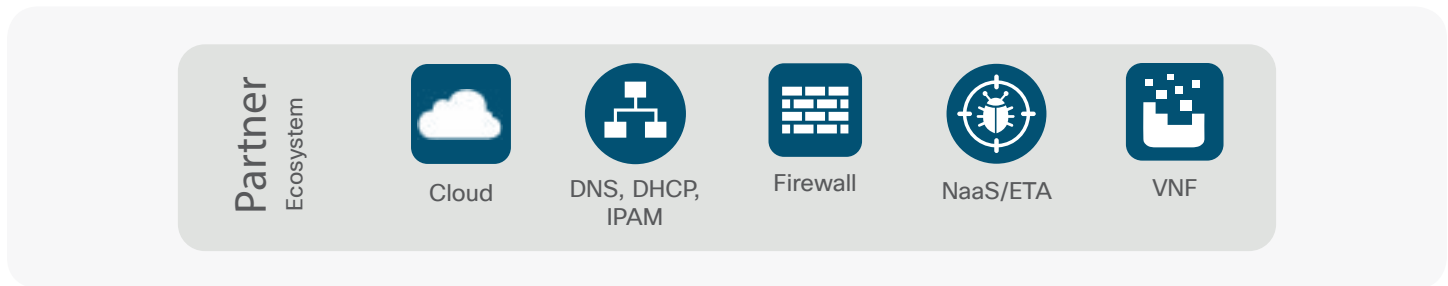
As more controller-based systems (from Cisco and our partners) are developed, and as advances are made in the hardware and software capabilities of fabric-enabled network devices, it is now possible to share real-time contextual information between Cisco DNA Center and various partner systems.

While the list continues to grow, here are a few examples:

· **Firewalls:** Share identity and policy content for group-based firewall rules.

· **DNS, DHCP and IPAM:** Share IP and name allocation of address pools.

  - Domain Name Services (DNS)

  - Dynamic Host Configuration Protocol (DHCP)

  - IP Address Management (IPAM)

· **Cloud Services:** Share identity, policy and forwarding context for cloud-based applications.

· **NaaS and ETA:** Share ID and policy attributes to mitigate threats.

  - Network as a Sensor (NaaS)

  - Encrypted Threat Analytics (ETA)

· **Virtual Network Functions (VNFs):** Share identity, policy and forwarding context for container-based applications.

There are many other examples and possibilities. As the Cisco SD-Access partner ecosystem continues to evolve, we will add new ways to share and use contextual data with our partners.

For more details, refer to the partner ecosystem section.

Physical layer

While Cisco SD-Access is designed for user simplicity, abstraction and virtual environments, everything runs on top of physical network devices, ports, and links. This section describes the network devices and operating systems that support Cisco SD-Access, why they are supported, and how they will support the solution as it evolves.

All Cisco network devices that actively participate in the SD-Access fabric must support all of the hardware (Application-Specific Integrated Circuits [ASIC] and Field-Programmable Gate Arrays [FPGA]) and/or software (protocols) requirements noted in the network layer section.

Cisco network devices (in particular, access-layer switches) that do not actively participate in the SD-Access fabric, but are connected to it via automation, are referred to as SD-Access extension nodes (see Table 2).

Refer to following link for the latest recommended software versions:
www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html

Cisco switches

Cisco switches provide the primary LAN (wired) access network elements. Multiple types of Cisco Catalyst® and Nexus® switches are available. Selection of the type(s) will depend on the interface type, bandwidth, scale, and environmental requirements of your physical network.

Table 1 lists Cisco switches supported as SD-Access fabric nodes.

Table 1.   Switch devices that SD-Access supports

Switch	Fabric role	Operating system (minimum)
Cisco Catalyst 9300 Series	Fabric edge*	Cisco IOS XE 16.6.1
Cisco Catalyst 9400 Series	Fabric edge*	Cisco IOS XE 16.6.1
Cisco Catalyst 9500 Series	Fabric border and control	Cisco IOS XE 16.6.1
Cisco Catalyst 3650 Series	Fabric edge*	Cisco IOS XE 16.6.1
Cisco Catalyst 3850 Series	Fabric edge*	Cisco IOS XE 16.6.1
Cisco Catalyst 4500-E Series • Supervisor Engine 8-E or 9-E	Fabric edge	Cisco IOS XE 3.10.0E
Cisco Catalyst 6880-X Series	Fabric border and control	Cisco IOS 15.4(1)SY2
Cisco Catalyst 6840-X Series	Fabric border and control	Cisco IOS 15.4(1)SY2
Cisco Catalyst 6807-XL • Supervisor Engine 2T or 6T • 6800 Series cards	Fabric border and control	Cisco IOS 15.4(1)SY2
Cisco Catalyst 6500-E Series • Supervisor Engine 2T or 6T • 6800 Series Cards	Fabric border and control	Cisco IOS 15.4(1)SY2
Cisco Nexus 7700 Series • Supervisor Engine 2E • M3 Series Cards	Fabric border	Cisco NxOS 8.2(1)

* Cisco Catalyst 9300 and 9400 Series and 3650 and 3850 Series also support fabric border, with limited capacity.

Table 2 lists switch devices that are supported as SD-Access extension nodes.

Table 2.   Switches supported as SD-Access extension nodes

Switch	Fabric role	Operating system (minimum)
Cisco Catalyst 3560-CX Series	Extension	Cisco IOS 15.2(6)E
Cisco Catalyst Digital Building Series	Extension	Cisco IOS 15.2(6)E
Cisco Industrial Ethernet 4000 and 5000 Series	Extension	Cisco IOS 15.2(6)E

For general information about Cisco switch platforms, refer to the following link: https://www.cisco.com/c/en/us/products/switches/index.html.

Cisco routers

Cisco routers provide the primary WAN and branch access network elements. Multiple types of Cisco ASR, ISR and CSR routers are available. Selection of the type(s) will depend on the interface type, bandwidth, scale, and environmental requirements of your physical network.

Table 3 lists the Cisco router devices supported as SD-Access fabric nodes.

Table 3.   Router devices that SD-Access supports

Router	Fabric role	Operating system (minimum)
Cisco ASR 1000-X Series	Fabric border and control	Cisco IOS XE 16.6.1
Cisco ASR 1000-HX Series	Fabric border and control	Cisco IOS XE 16.6.1
Cisco ISR 4300 Series	Fabric border and control	Cisco IOS XE 16.6.1
Cisco ISR 4400 Series	Fabric border and control	Cisco IOS XE 16.6.1
Cisco Integrated Services Virtual Router (ISRv)	Fabric border and control*	Cisco IOS XE 16.6.1
Cisco Cloud Services Virtual Router (CSRv)	Fabric control*	Cisco IOS XE 16.6.1

* Software (VM) based devices must meet minimum physical (appliance) and network layer requirements.

For general information about Cisco router platforms, refer to the following link: https://www.cisco.com/c/en/us/products/routers/index.html.

Cisco wireless

Cisco wireless LAN controllers and access points provide the primary WLAN (wireless) access and network elements. Many types or controllers and access points types are available, with a focus on 802.11ac models. Selection will depend on the bandwidth, scale, and environmental requirements of your wireless network.

Table 4 lists the Cisco wireless devices supported as SD-Access wireless controller nodes.

Table 4. Wireless devices that SD-Access supports

Router	Fabric role	Operating system (minimum)
3504 Wireless Controller	Fabric WLAN controller	AireOS 8.5.103.0
5520 Wireless Controller	Fabric WLAN controller	AireOS 8.5.103.0
8510 Wireless Controller	Fabric WLAN controller	AireOS 8.5.103.0
8540 Wireless Controller	Fabric WLAN controller	AireOS 8.5.103.0

Table 5 lists the Cisco wireless devices supported as SD-Access access point nodes.

Table 5. Access points that SD-Access supports

Access point	Fabric role	Operating system (minimum)
Aironet® 1700 Series	Fabric access point*	AireOS 8.5.103.0
Aironet 2700 Series	Fabric access point*	AireOS 8.5.103.0
Aironet 3700 Series	Fabric access point*	AireOS 8.5.103.0
Aironet 1800 Series	Fabric access point	AireOS 8.5.103.0
Aironet 2800 Series	Fabric access point	AireOS 8.5.103.0
Aironet 3800 Series	Fabric access point	AireOS 8.5.103.0

* Aironet 1700, 2700, and 3700 Series Wave 1 access points have some hardware caveats. Refer to the release notes.

For general information about Cisco wireless platforms, refer to the following link: https://www.cisco.com/c/en/us/products/wireless/index.html.

Cisco appliances

For simplicity, there are only two types of appliances to consider: Cisco DNA Center and ISE.

Note: Additional appliances may be introduced at a later time. Refer to the appliance release notes.

Table 6 lists the Cisco DNA Center hardware appliance(s).

Table 6. Cisco DNA Center hardware appliances

Appliance	Fabric role	Operating system (minimum)
Cisco DNA Center	Cisco DNA Center controller	Cisco DNA Center 1.0

For general information about the Cisco DNA Center appliance(s), refer to the following link: https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html.

Table 7 lists the Cisco ISE hardware appliance(s).

Table 7.   Cisco ISE hardware appliances

Appliance	Fabric role	Operating system (minimum)
Cisco Secure Network Server 3500 Series	Cisco ISE controller	ISE 2.3

Note: Cisco ISE supports both VM and appliance deployment models (for different design and scale requirements). The ISE appliances noted above are recommended for a complete SD-Access deployment.

For general information about the Cisco ISE appliance(s), refer to the following link: https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html.

Network layer

As noted earlier, the network layer consists of two sublayers: network underlay and fabric overlay. These two sublayers form the "access" and "fabric" aspects of the overall SD-Access solution (in a traditional networking sense), and they work together to deliver the data packets to and from the network devices participating in SD-Access. All of this network layer information is made available to the controller layer.

As the names suggest, the network underlay runs "under" the fabric overlay, and the overlay runs "over" the underlay. This provides a clear separation of responsibilities and maximizes the capabilities of each sublayer.

The **network underlay** is analogous to your existing Layer 2/Layer 3 network and is most closely associated with the physical layer, but with a simplified focus on transporting data packets between network devices for the (logical) overlay. The **fabric overlay** is mostly a logical (tunneled) network that virtually interconnects all of the network devices (to form a "fabric"). This abstracts the inherent complexities and limitations of the (physical) underlay.

Note: Network devices may participate in only one network sub-layer function (e.g. intermediate devices) or both (e.g. fabric-enabled devices), but it is important to consider them separately.

Figure 8 shows a visual representation of the relationship between the fabric overlay and network underlay.

Figure 8.   Relationship between fabric overlay and network underlay
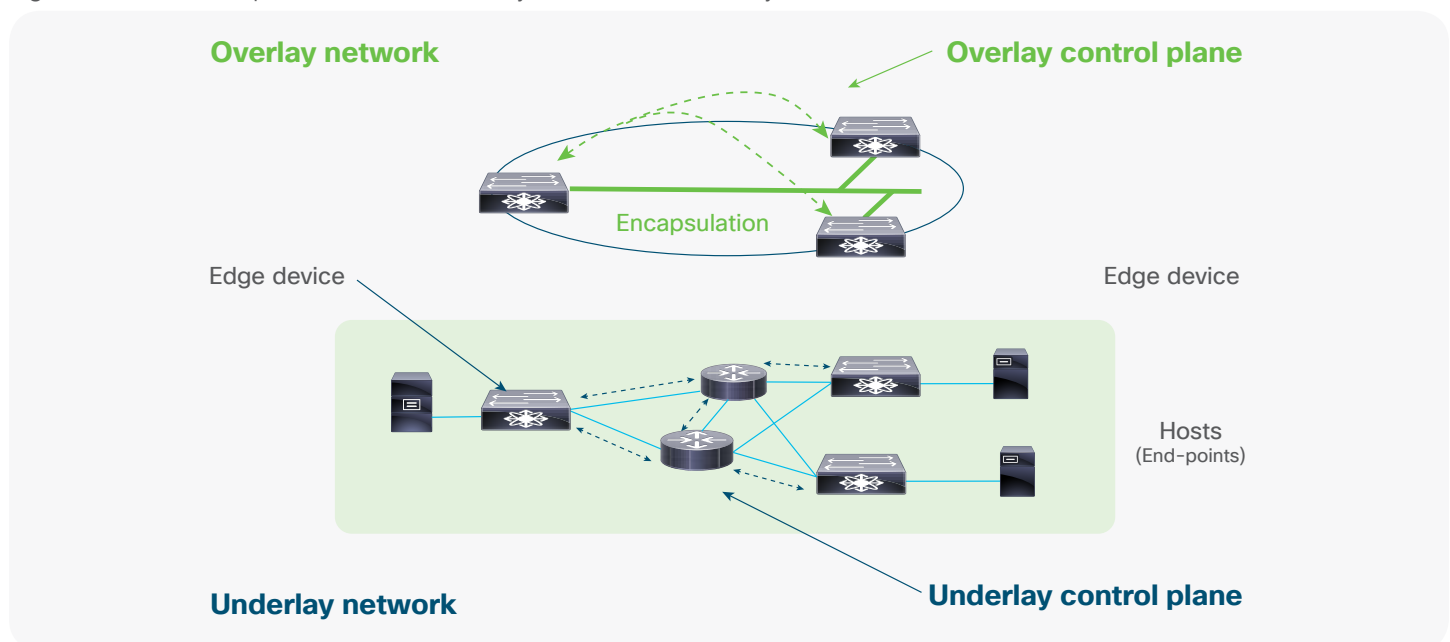
Network underlay

The network underlay should be designed for maximum simplicity and resiliency. This includes all standard physical-layer best practices for hardware redundancy, multiple data paths, etc. as well as standard network-layer best practices for protocol redundancy, timers, control-plane protection, etc.

Note: It is technically possible to use a Layer 2 (Spanning Tree Protocol [STP]) network underlay design, but it is not recommended. The recommended design for the network underlay is to use a Layer 3 (Interior Gateway Protocol [IGP]) routing environment.

Note: Any problem(s) with the network underlay may affect operation of the fabric overlay.

Two models of network underlay are supported:

- **Custom underlay:** Either an existing network or a network configured and managed manually (such as with a CLI or API) without the use of Cisco DNA Center.
- **Automated underlay:** A new, fully automated network underlay, whereby all aspects of the network are configured and managed by Cisco DNA Center.

Custom underlay

In a custom underlay, the user must provide all of the physical and logical interface address configurations, as well as all of the control-plane protocols and address configurations to provide full IP reachability between fabric-enabled network devices and Cisco DNA Center and Cisco ISE.

- The **main advantages** are that you are already familiar with your own environment (the interfaces, IP addresses, protocols, etc.), and are permitted to customize the operating behavior to fit your requirements. Another key advantage is that the fabric overlay is capable of running over the top of a legacy (or non-Cisco) IP-based network.
- The **main disadvantages** are that you are responsible for all configuration and management requirements, and any problem(s) may affect the operation of the fabric overlay. Some examples of custom underlay problems include improper IP addressing and/or routing, IP Time-To-Live (TTL), Maximum Transmission Unit (MTU) size and fragmentation, excessive latency and Round-Trip Time (RTT), etc.

Automated underlay

In an automated underlay, Cisco DNA Center manages the provisioning of all of the physical and logical interface address configurations, as well as all of the control-plane protocols and address configurations to provide full IP reachability between all fabric-enabled network devices and Cisco DNA Center and Cisco ISE.

- The **main advantages** are that you need only provide the necessary IP addresses to allow IP reachability to the external network. All other aspects of the network underlay (and fabric overlay) are fully automated, including configurations across multiple network layers. This eliminates misconfigurations and reduces the complexity of the network underlay. It also greatly simplifies and speeds the building of the network underlay.
- The **main disadvantages** are that you are no longer able to provide any customization (for special design requirements). The network underlay is built to meet a standard compliance design, to maximize operations. Also, the automated underlay tool does require that one "seed" device be configured manually to start, from which all others will be automated.

Note: The Cisco DNA Center automated underlay will provision a Layer 3 (IGP) routing environment.

Fabric overlay

The fabric overlay provides the infrastructure for building virtual networks with policy-based segmentation constructs, as well as providing dynamic host services for mobility and enhanced security, beyond the normal switching and routing capabilities.

The fabric overlay will be fully automated, regardless of the network underlay model used. This includes all necessary overlay control-plane protocols and addressing, as well as all global configurations associated with operation of the SD-Access fabric.

Note: The fabric overlay may also be manually configured and managed (via CLI and/or API), but this design model is commonly referred to as Campus Fabric.

As noted earlier, the Cisco SD-Access fabric is based on multiple existing (standard) technologies. You may already be familiar with one or all of them, and there is a wealth of existing reference information for each technology available online. Beyond that, it's the combination and automated management of these technologies that make Cisco SD-Access so powerful and unique.

There are three basic planes of operation in the fabric overlay:

- **Control plane:** Contains the settings, protocols, and tables for the fabric-enabled devices that provide the logical forwarding constructs of the fabric overlay.
- **Data plane:** A specialized IP/User Datagram Protocol (UDP)-based frame encapsulation that contains the forwarding and policy constructs for the fabric overlay (used by fabric-enabled devices).
- **Policy plane:** Contains the settings, protocols, and tables for the fabric-enabled devices that provide the policy constructs of the fabric overlay.

Fabric control plane

The primary technology used for the fabric control plane is based on the **Locator/ID Separation Protocol (LISP)** (Figure 9). LISP is an IETF standard protocol (RFC-6830, etc.) based on a simple endpoint ID (EID) to routing locator (RLOC) mapping system, to separate the "identity" (address) from its current "location" (attached router).

LISP dramatically simplifies traditional routing environments by removing the need for each router to process every possible IP destination address and route. It does this by moving remote destination information to a centralized map database that allows each router to manage only its local routes (and query the map system to locate destination endpoints).

This technology provides many advantages for Cisco SD-Access, such as less CPU usage, smaller routing tables (hardware and/or software), dynamic host mobility (wired and wireless), address-agnostic mapping (IPv4, IPv6, and/or MAC), built-in network segmentation (Virtual Routing and Forwarding [VRF]), and others.

In Cisco SD-Access, several enhancements to the original LISP specifications have been added, including distributed Anycast Gateway, Virtual Network (VN) Extranet and Fabric Wireless, and we will continue to add more capabilities in the future.

Figure 9.   Fabric control-plane based on LISP
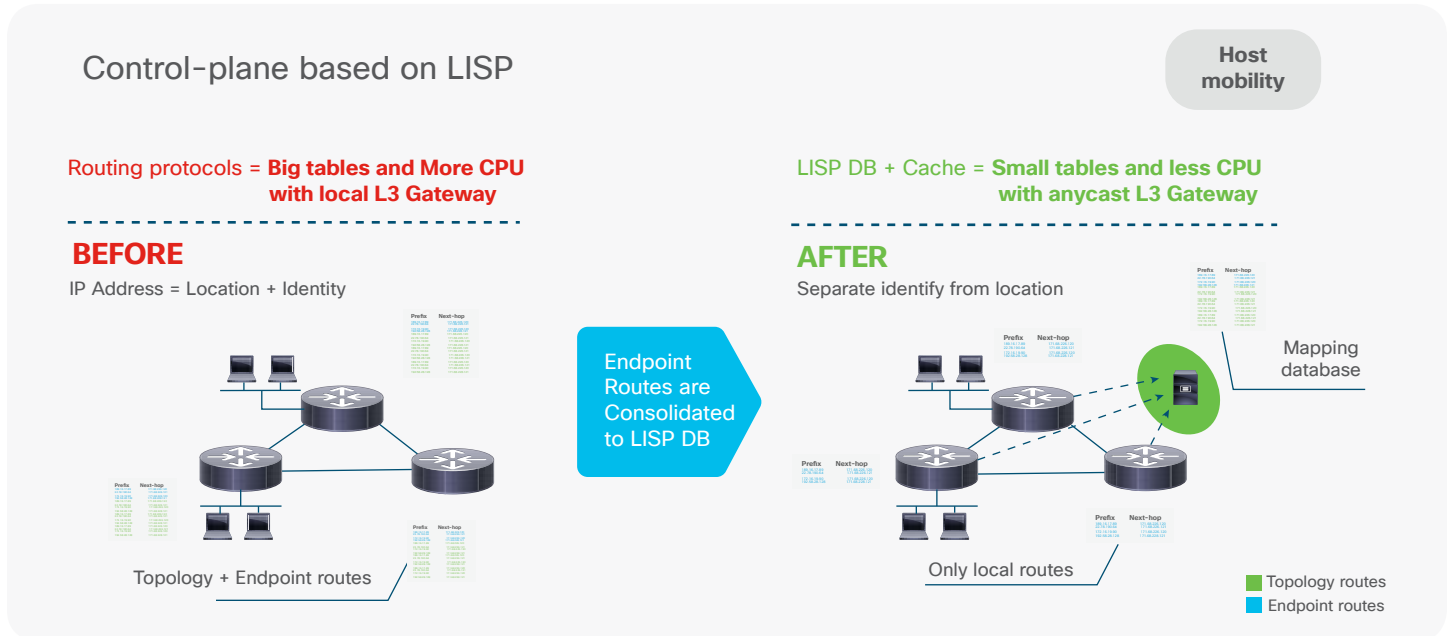
For more information about LISP, refer to the following links: https://www.cisco.com/go/lisp/ or http://tools.ietf.org/wg/lisp/.

Fabric data plane

The primary technology used for the fabric data plane is based on **Virtual Extensible LAN (VXLAN)** (Figure 10). VXLAN is an IETF standard encapsulation (RFC-7348, etc.).

VXLAN encapsulation is IP/UDP-based, meaning that it can be forwarded by any IP-based network (legacy or non-Cisco) and effectively creates the "overlay" aspect of the SD-Access fabric. VXLAN encapsulation is used (instead of LISP encapsulation) for two main reasons. VXLAN includes the source Layer 2 (Ethernet) header (LISP does not), and it also provides special fields for additional information (such as virtual network [VN] ID and group [segment] ID).

This technology provides several advantages for SD-Access, such as support for both Layer 2 and Layer 3 virtual topologies (overlays), and the ability to operate over any IP-based network with built-in network segmentation (VRF/VN) and built-in group-based policy.

In SD-Access, some enhancements to the original VXLAN specifications have been added, most notably the use of security group tags (SGTs). This new VXLAN format is currently an IETF draft known as Group Policy Option (or VXLAN-GPO).

Note: VXLAN-GPO is discussed further in the Fabric Policy Plane section.

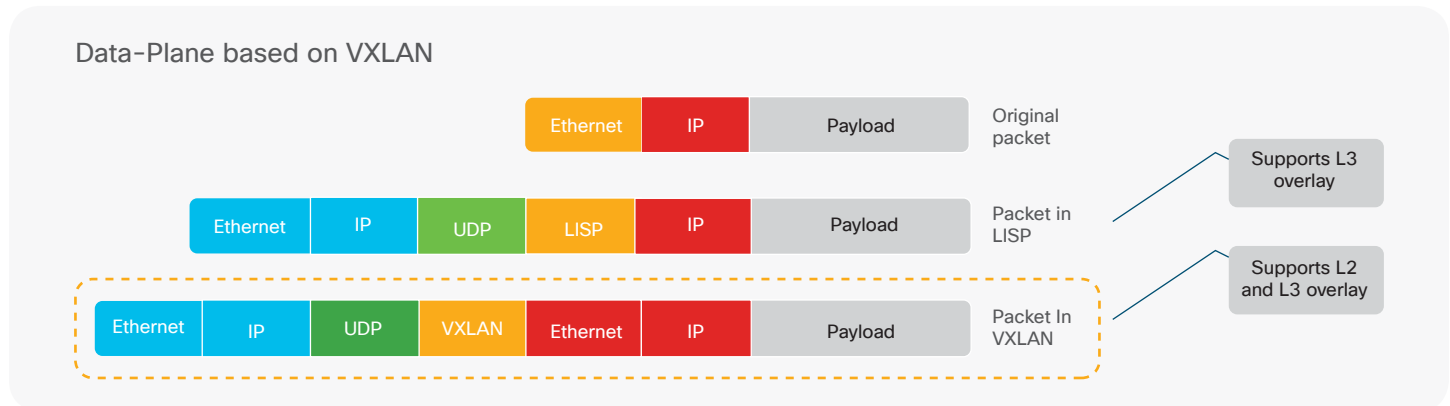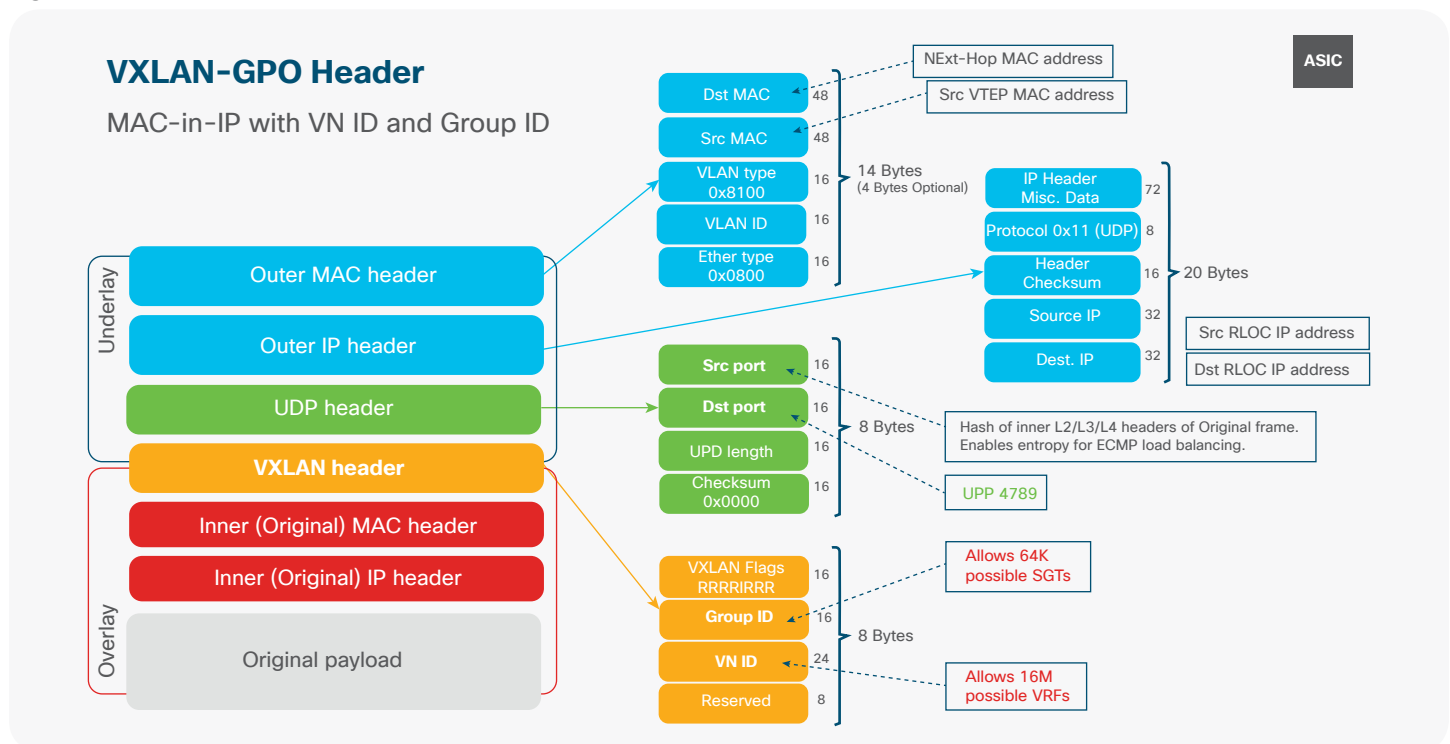Figure 10. Fabric data plane based on VXLAN

Figure 11 shows a visual representation of how VXLAN-GPO is used in Cisco SD-Access.

Figure 11. How VXLAN-GPO is used in SD-Access

For more information about VXLAN (or GPO), refer to the following link(s): https://tools.ietf.org/html/rfc7348 or https://tools.ietf.org/html/draft-smith-vxlan-group-policy-03.

Fabric policy plane

The primary technology used for the fabric policy plane is based on **Cisco TrustSec®** (Figure 12). Cisco TrustSec, and specifically SGT and SGT Exchange Protocol (SXP), is an IETF draft protocol (SXP-006) that provides logical group-based policy creation and enforcement by separating the actual endpoint "identity" (group) from its actual network address (IP) using a new ID known as a Scalable [or security] Group Tag (SGT).

An SGT is a unique (16-bit) ID tag, separate from the network address. This allows the user to create network policies (such as security, Quality of Service [QoS], Policy-Based Routing [PBR], etc.) based solely on the SGT, regardless of the actual location. Also, when SGTs and VNs are combined together, we can create a two-level hierarchical policy model. SGTs (along with VNs) allow you to create different levels of network-based (VNID) and/or group-based (SGT ID) segmentation.
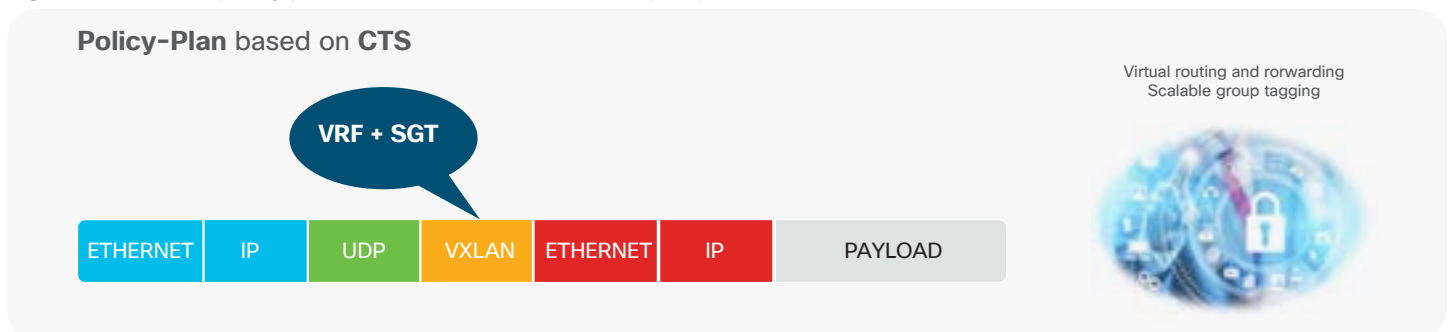
Note: VRF (VN) is actually a forwarding construct, and not normally associated with Cisco TrustSec. It is included here to demonstrate how Cisco TrustSec with VNID are used within SD-Access to provide a two-level segmentation solution.

This technology provides several advantages for Cisco SD-Access, such as support for both network-based (VRF/ VN) and group-based segmentation (policies), the ability to create logical (address-agnostic) policies, dynamic enforcement of group-based policies (regardless of location) for both wired and wireless traffic, and the ability to provide policy constructs over a legacy or non-Cisco network (using VXLAN-GPO).

In SD-Access, several enhancements to the original Cisco TrustSec specifications have been added, notably combining the SGT and VN into the VXLAN-GPO header and enhancing Cisco TrustSec to include LISP VN Extranet, and we will continue to add more capabilities in the future.

Note: Remember that it's the new VXLAN-GPO encapsulation that carries the SGT and VNID.

Figure 12.   Fabric policy plane based on Cisco TrustSec (CTS)

For more information about Cisco TrustSec (and SGTs), refer to the following link(s): https://www.cisco.com/go/ trustsec/ or https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/.

Fabric roles

The operation of the fabric overlay requires several different device roles, each with a specific set of responsibilities. Each fabric-enabled network device (they are configured for both network underlay and fabric overlay operation) must be configured for one (or more) of these roles.

During the planning and design process, it is important to understand the fabric roles and to select the most appropriate network device(s) for each role. This document will not cover design-specific details, but a clear understanding of the basic purpose and operation of each role will help make the design-specific requirements clear.

For more information on SD-Access design and deployment, please refer to the following link(s): https://www.cisco. com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Guide-2017AUG.pdf.

There are four basic device roles in the fabric overlay:

- **Control plane node:** Contains the settings, protocols, and tables to provide the endpoint-to-location mapping system for the fabric overlay.
- **Fabric border node:** Contains the settings, protocols, and tables to provide internal and external routing between the fabric overlay and outside networks.

- **Fabric edge node:** Contains the settings, protocols, and tables, to provide (wired) endpoint onboarding and host mobility for the fabric overlay.
- **Fabric WLAN controller (WLC):** Contains the settings, protocols, and tables to provide (wireless) endpoint onboarding and host mobility for the fabric overlay.

A **control plane** node maintains a simple host tracking database to map endpoints to location information. It is based on a LISP map server/resolver, but has been enhanced for SD-Access functions such as fabric wireless, SGT mapping, etc.

The control plane (host database) maps all endpoint ID (EID) locations to the current fabric edge or border node. It is capable of multiple EID lookup types (IPv4, IPv6, or MAC). IPv4 EIDs are supported in the initial release, with IPv6 and MAC EIDs being added later (Figure 13).

The control plane then services map registrations from fabric edge or border nodes for "known" EID (IP) prefixes, and resolves lookup requests from fabric edge or border nodes to locate destination EIDs.

Note: Control plane devices must maintain all endpoint (host) mappings in a fabric. Select a device with sufficient hardware and software scale for the fabric.

A control plane node must be either a Cisco switch or a router operating in the fabric overlay.

Figure 13.   Fabric control plane node
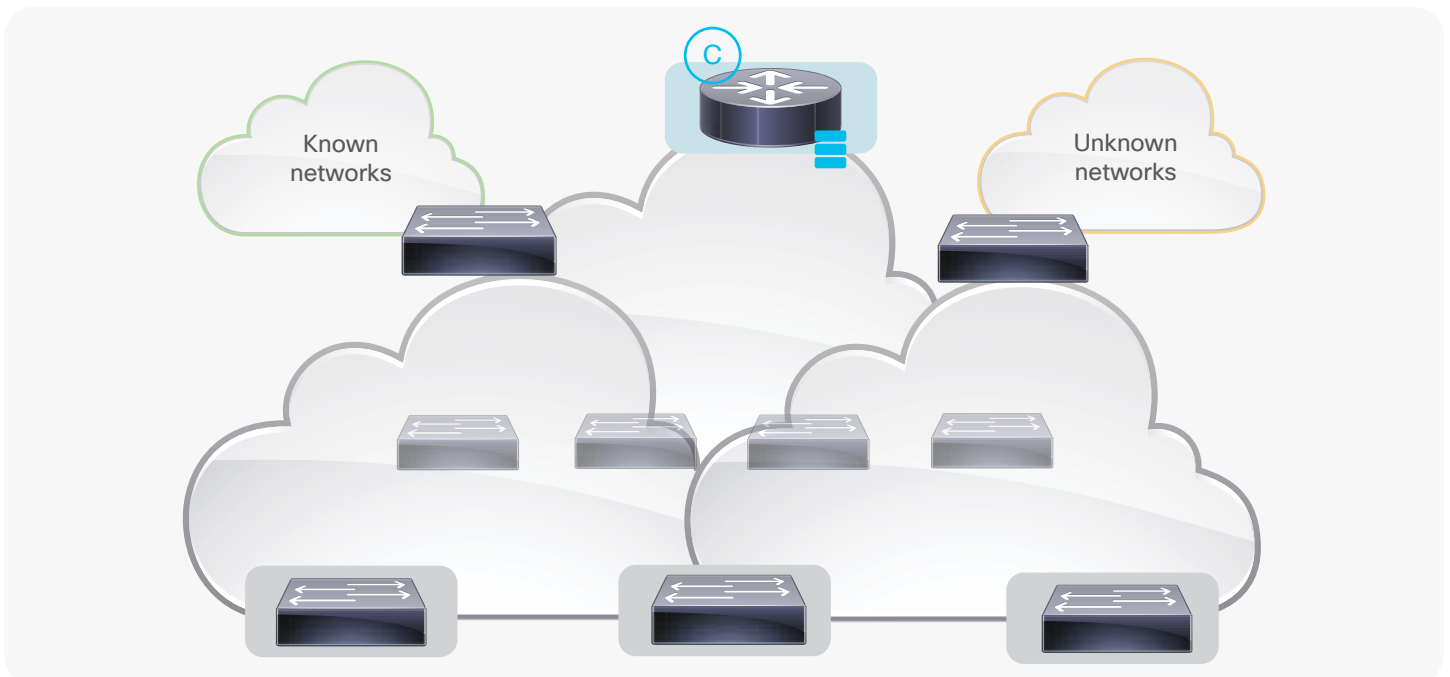
There are two types of fabric border node: **fabric border** and **default border**. Both types provide the fundamental routing entry and exit point for all data traffic going into and out of the fabric overlay, as well as for VN and/or group-based policy enforcement (for traffic outside the fabric).

A fabric border is based on a LISP XTR, and is used to add "known" IP/mask routes to the map system. A known route is any IP/mask that you want to advertise to your fabric edge nodes (for example, remote WLC, shared services, data center, branch, private cloud, etc.). A default border is based on a LISP PXTR, and is used for any "unknown" routes (such as Internet or public cloud) as a gateway of last resort (Figure 13).

Note: Both types of fabric border nodes can coexist in the same fabric. Only two default borders are allowed per fabric.

A fabric border **both exports and advertises** fabric IP/mask routes, and **also imports and advertises** outside IP/mask entries into the map system (Figure 14).

A default border **only exports** fabric IP/mask routes, but does not import (map) anything from outside. It's based on a default entry, if no other map entry exists (lookup miss).

Note: Border devices must maintain both the inside (fabric) and outside (non-fabric) routes. Select a device with sufficient hardware and software scale for the fabric.

It is possible for a device to be both a regular fabric border and a default border at the same time.[*]

[*] Cisco Nexus 7700 switches support only default borders as of NxOS 8.2(1).

Figure 14.   Fabric border and default border nodes
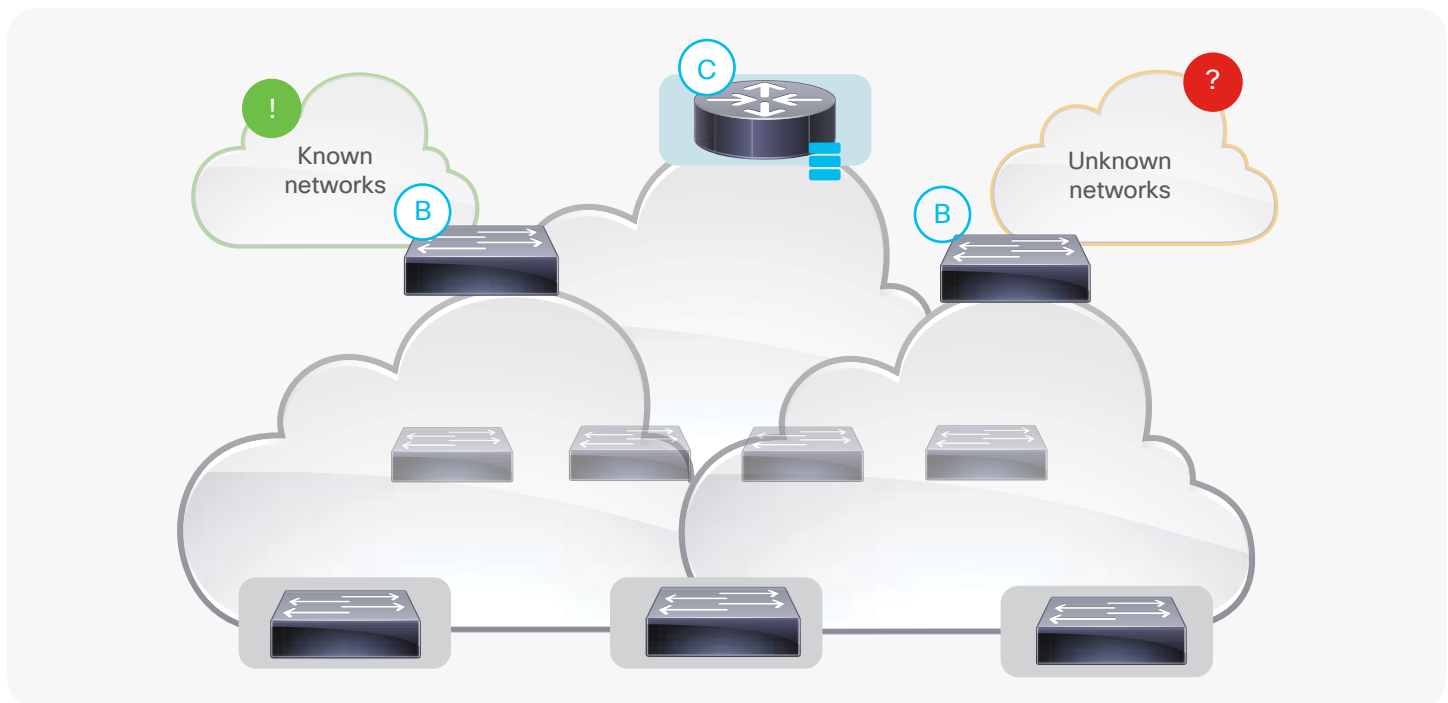
A **fabric edge** node provides onboarding and mobility services for wired users and devices (including fabric-enabled wireless controllers and access points) connected to the fabric. It is based on a LISP XTR with dynamic EID mapping and Anycast Gateway, and also provides endpoint authentication and assignment to overlay host pools (static or DHCP), as well as group-based policy enforcement (for traffic to fabric endpoints).

A fabric edge first identifies and authenticates wired endpoints (such as static, 802.1X, and Active Directory), in order to place them in an address pool (switch virtual interface [SVI] and VRF) and scalable group. It then registers the specific EID host address (such as /32 or /128) with the control plane node (Figure 15).

A fabric edge provides a single Layer 3 Anycast Gateway (same IP address on all edge nodes) for its connected endpoints, and also performs the encapsulation and de-encapsulation of host traffic to and from its connected endpoints.

Note: An edge node must be either a Cisco switch or router operating in the fabric overlay.

Figure 15.   Fabric edge nodes
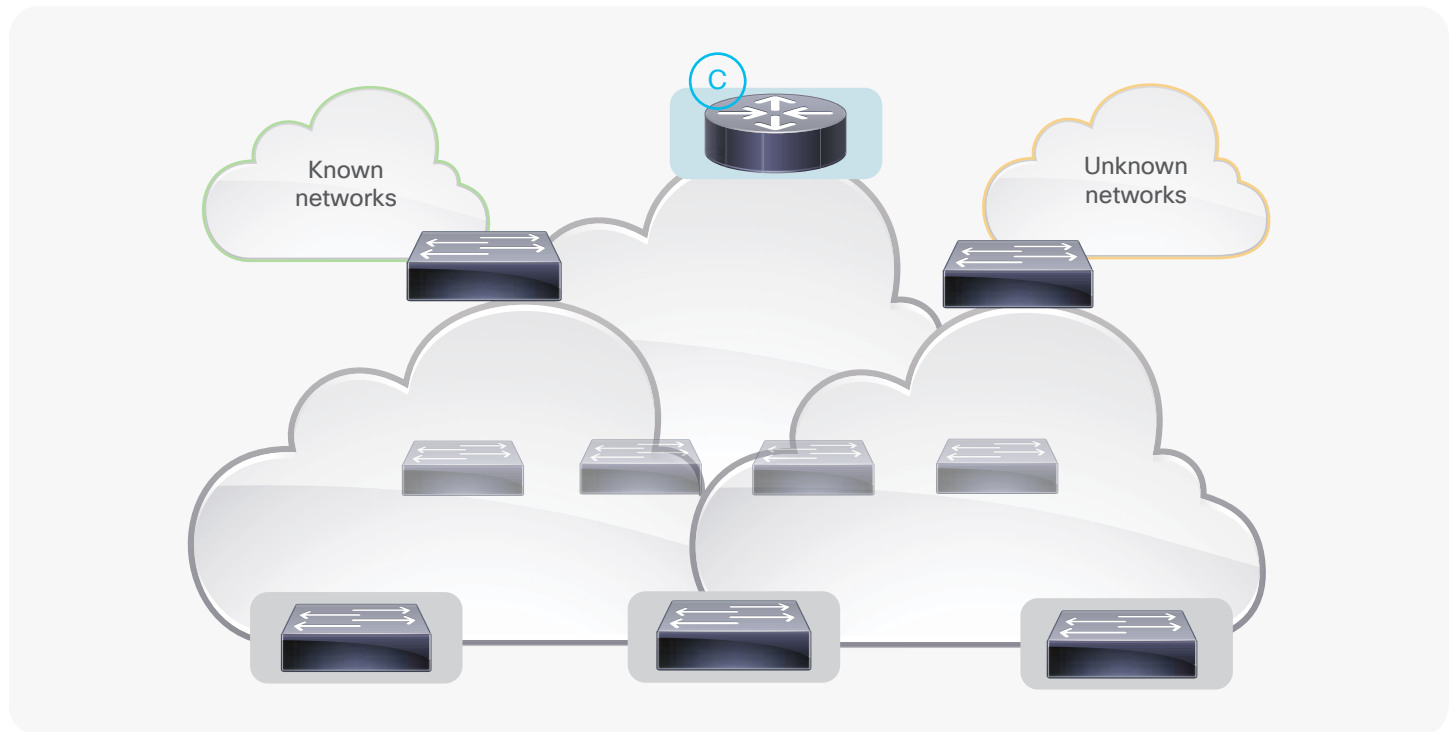
A **fabric WLC** node provides onboarding and mobility services for wireless users and devices connected to the fabric. A fabric WLC also performs proxy XTR registrations to the control plane (on behalf of the fabric edges), and can be thought of as a special fabric edge for wireless clients. The control plane then maps the host EID to the current fabric access point (and the connected fabric edge node) location.

A fabric WLC connects to the SD-Access fabric via a fabric border node (in the underlay). Fabric access points register to the fabric WLC via the Control and Provisioning of Wireless Access Points (CAPWAP) protocol, using a dedicated access point host pool (in the overlay). Fabric access points connect directly to the fabric edge via VXLAN (Figure 16).

Wireless clients (SSIDs) use regular host pools for traffic and policy enforcement (same as wired). The fabric WLC then registers client EIDs with the control plane node (as located on the edge).

Note: A fabric WLC is connected outside the fabric (single hop or multihop) via a fabric border node (in the underlay).

A fabric access point must be directly connected to a fabric edge node (in the overlay).

Figure 16.   Fabric wireless LAN controller
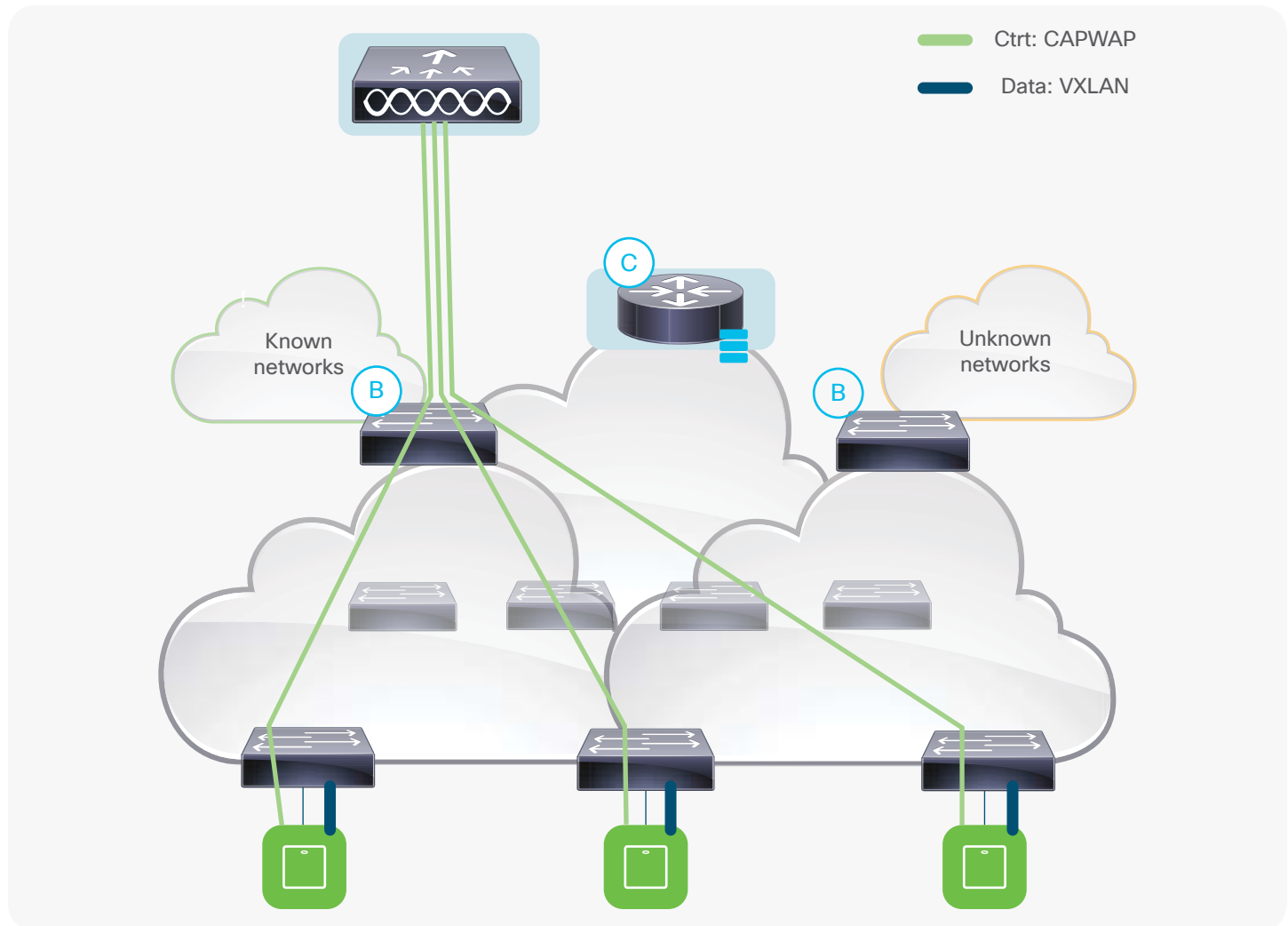
For more information on SD-Access Wireless, refer to the following link: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/few.pdf.

Fabric constructs

To understand the benefits and operation of Cisco SD-Access, you must be aware of several important concepts (or constructs). As noted earlier, the SD-Access fabric is based on multiple existing (standard) technologies, which you may already be familiar with, but it is important to understand how they operate and interact in SD-Access.

There are three basic constructs in the fabric overlay:

- **Virtual network:** Provides a unique (and isolated) routing and switching forwarding construct for network-based segmentation policies.
- **Security group:** Provides a unique (address-agnostic) endpoint grouping construct for group-based segmentation policies.
- **Host (address) pool:** Provides the necessary IP address/mask information for SD-Access endpoints to route to non-fabric environments.

A **virtual network** is a separate routing and switching table instance to isolate host pools. It's based on VRF, with the same basic purpose and rules as in traditional networks. SD-Access (with its LISP-based control plane) assigns every endpoint (host) to a virtual network (including the Default_VN). Communication between endpoints in different VNs must traverse a firewall and/or VRF router. SD-Access 1.1 also provides LISP VN Extranet, for remote location resolution across VNs. Assignment to a VN is based on the associated host pool, discussed later.

The same VN (VRF) is configured on all fabric edge and border nodes. The control plane node uses instance IDs to maintain separate VRF tables (Default_VN is instance ID "4097"). EID prefixes (host pools) are then registered within a VN. If VN Extranet is used, it adds the VNID to the EID location mapping (Figure 17).

The fabric edge and border nodes include the VNID in each VXLAN header, which is then carried across the fabric. This keeps each VN separate and allows VRF-based routing and/or firewall policy and enforcement.

Fabric border nodes use standard "vrf definition," with "route-distinguisher" and "route-target" (import/export) configurations for remote VRF advertisement (to external networks).

Figure 17. Fabric virtual networks
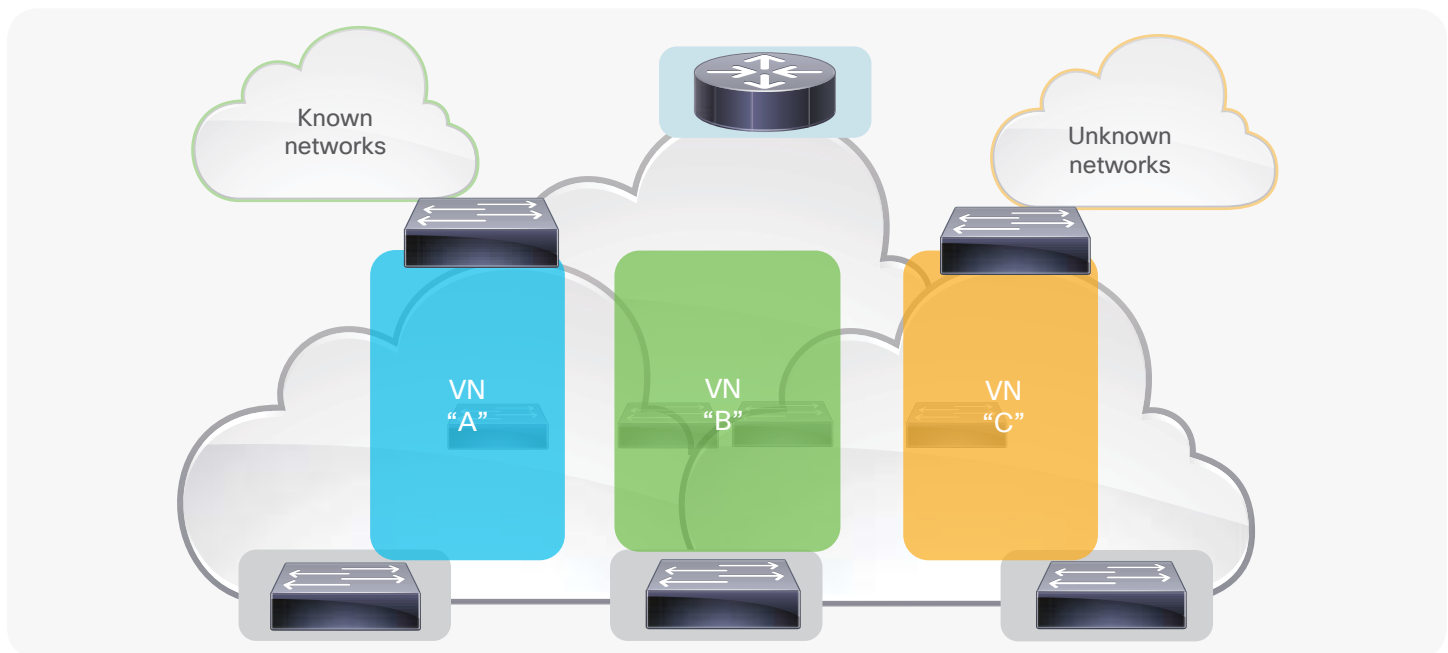
Note: VN is currently a "global" construct in SD-Access. This means that the fabric-enabled device with the lowest number of VRF entries (per-domain) will determine the per-domain scale limit. Select devices with sufficient VRF scale to support your fabric.

A **scalable group** is a logical object to "group" similar endpoints (with similar policies). It's based on an SGT, with the same basic purpose and rules as in traditional networks. Cisco SD-Access (with its Cisco TrustSec-based policy plane) assigns every endpoint (host) to a scalable group. Assignment to a scalable group can be either static (per fabric edge port) or via dynamic authentication (authentication, authorization, and accounting [AAA] or RADIUS via Cisco ISE).

The same scalable group is configured on all fabric edge and border nodes (Figure 18). Groups can be defined in Cisco DNA Center and/or Cisco ISE and are advertised via Cisco TrustSec. There is a direct (1-to-1) relationship between host pools (below) and scalable groups. Thus, the scalable groups operate within a VN by default.

The fabric edge and border nodes include the SGT ID in each VXLAN header, which is carried across the fabric. This keeps each scalable group separate, and allows SGT-based access control list (SGACL) policy and enforcement.

Figure 18.   Fabric scalable groups
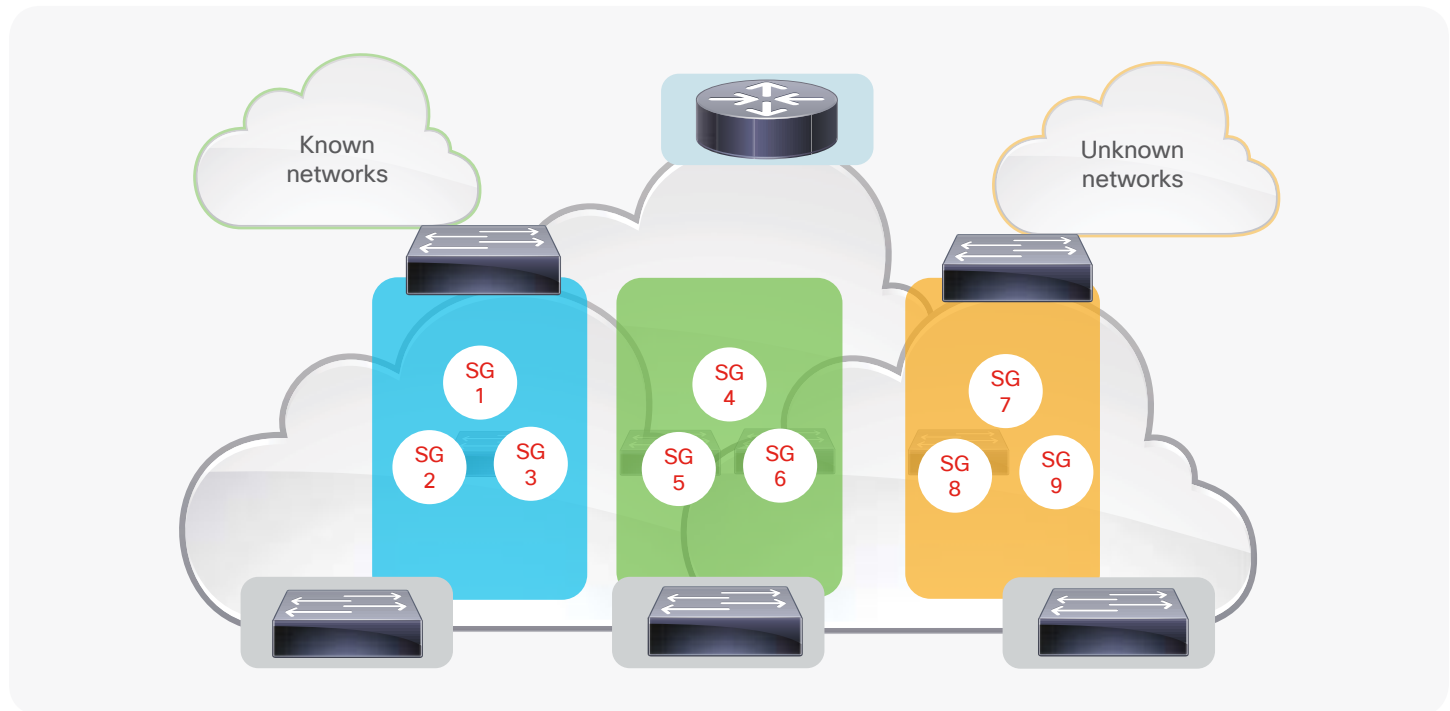
Note: Up to 64,000 (software) scalable groups are permitted in Cisco SD-Access, but fabric-enabled devices support a different number of (hardware) SGACLs. SGACLs are applied to a fabric-enabled device only when a host is present. Select devices with sufficient SGACL scale to support your fabric.

A **host (address) pool** provides onboarding and IP address services to endpoints. It's based on an SVI with Anycast Gateway, with the same purpose and rules as in traditional networks. Cisco SD-Access assigns every endpoint to a host pool (and the associated VN) (Figure 19). Host IP addresses can be static (per host) or provided via DHCP. Assignment to a host pool can be either static (per port), or via dynamic authentication (AAA/RADIUS via Cisco ISE).

The same anycast IP (SVI) is configured on all fabric edge nodes. The SVI is also enabled for LISP dynamic EIDs, to register host-specific addresses (i.e. /32 or /128) and their associated VN to the control plane.

Cisco SD-Access provides a new DHCP relay capability to support VRF-based IP scopes, without modifying DHCP servers. Fabric edge nodes relay DHCP requests to the fabric border (advertising the DHCP server IP). The border stores the edge node (source RLOC IP) to return DHCP offers to the requesting host.

Figure 19. Fabric host pools
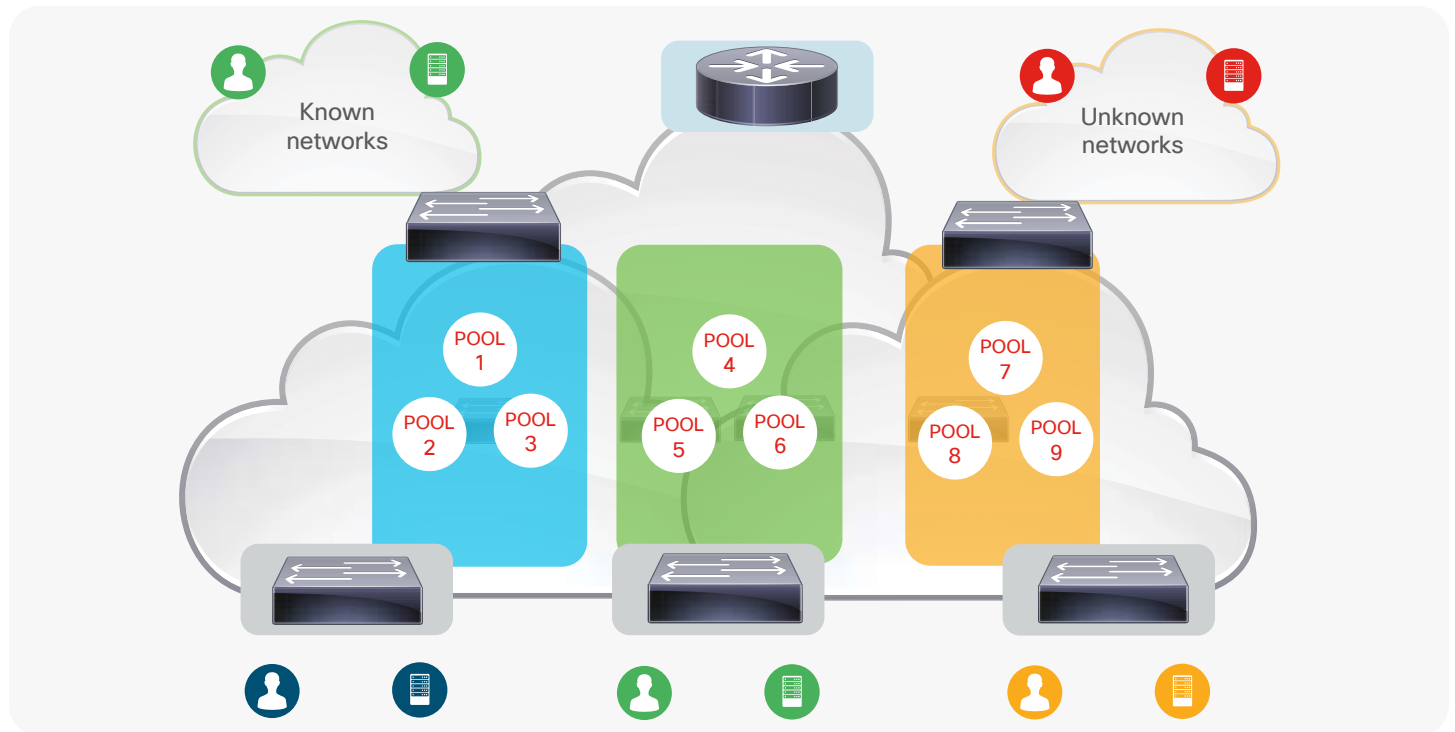
Note: All host address pools (and per-host entries) are known by the control plane node(s). Select control plane devices with sufficient address scale to support your fabric.

Controller layer

The controller layer provides all of the management subsystems for the management layer (and partner ecosystem) (Figure 20). These are the physical server appliances noted in the physical layer section.

Figure 20. The controller layer
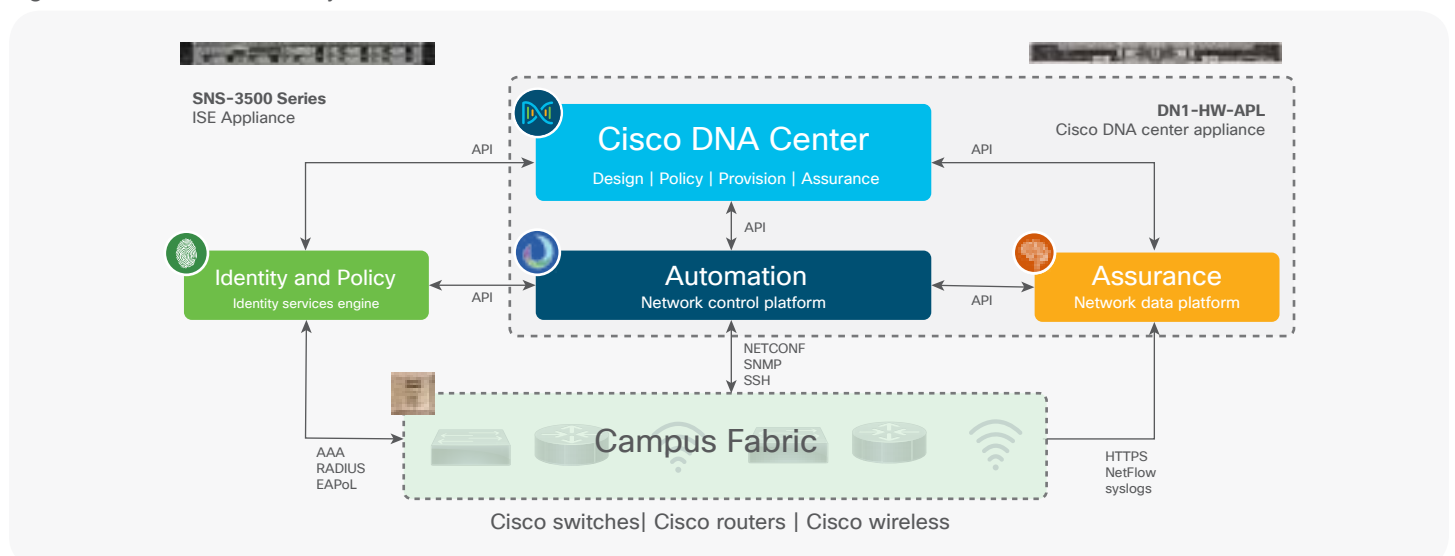
As noted earlier, these controller subsystems are effectively the work being done behind the scenes, to abstract the complexities and dependencies of managing so many network devices. Together, they provide a complete "closed-loop" management environment for all aspects of your Cisco SD-Access network.

There are three main controller subsystems:

- **Cisco NCP:** Contains the settings, protocols, and tables to automate management of the network underlay and fabric overlay (wired and wireless).
- **Cisco NDP:** Contains the settings, protocols, and tables to monitor and analyze hosts and devices in the network underlay and fabric overlay (wired and wireless).
- **Cisco ISE:** Contains the settings, protocols, and tables to provide identity and policies for the network underlay and fabric overlay (wired and wireless).

All of the base and fabric automation services are provided by **Cisco NCP,** and all of the analytics and assurance services are provided by **Cisco NDP**. Both of these subsystems run together on the same physical appliance(s): Cisco **DNA Center**.

All of the identity and policy services are provided by the **Cisco ISE**, which runs on a separate appliance(s): Cisco Secure Network Server Series.

These controller subsystems may be run on single- or multiple-server appliances in a standalone, redundant, or distributed model, on-premises or (in the future) as cloud-based services.

Cisco NCP

Cisco Network Controller Platform (NCP) The subsystem integrates directly with the Cisco ISE and NDP subsystems to provide contextual automation information between them. This is done through various API-based data exchange mechanisms, as well as automated certificate exchange for partner systems (for example, Cisco ISE). All of this information is then provided back to the user (management layer).

Note: All of the Cisco NCP software is included with the Cisco DNA Center appliance.

Figure 21.   Cisco NCP (embedded within Cisco DNA Center)
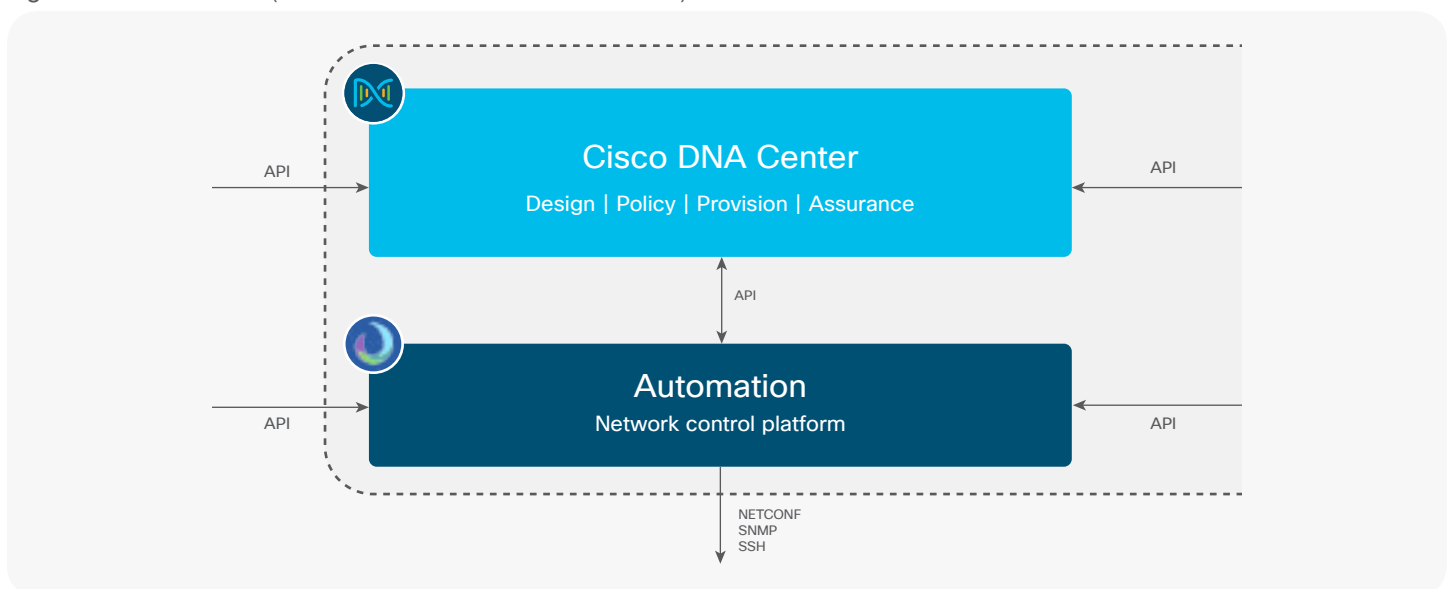
The basic role of NCP is to provide all of the base (that is, global and non-fabric [underlay]) and fabric automation and orchestration services for the physical layer and network layer. NCP is capable of communicating with the Cisco network devices in a variety of forms, including NETCONF/YANG, Simple Network Management Protocol (SNMP), SSH/Telnet, etc.

NCP then uses one or all of these communication methods to configure and manage all of the network devices, and then provide network automation status and other information back to the management layer.

Note: Many of the NCP functions are available via published APIs. This enables external systems to interact with and/or augment NCP. Refer to the partner ecosystem section for more information.

The various NCP services run as software packages (which can be added and upgraded independently) that share contextual data among themselves, with each processing specific functions within the overall subsystem. These services are then exposed to the management layer as various UI applications and/or workflows.

Cisco NCP is responsible for two primary services (apps) in Cisco DNA Center 1.0:

- **Cisco DNA Design:** Provides the base-level workflows, as well as site profiles, maps and floorplans, network settings, IP address management, wireless, etc.
- **Cisco DNA Provision:** Provides the SD-Access workflows, including device provisioning, fabric domains, device roles, host onboarding, etc.

In addition, the following other NCP services (apps) are available in Cisco DNA Center 1.0:

- **Device Discovery:** Discovers existing Cisco routers, switches, and wireless controllers.
- **Device Inventory:** Maintains network and host details, configurations, and software versions.
- **Plug-and-Play (PnP):** Automates deployment of Cisco routers, switches, and wireless controllers.
- **Path Trace:** Creates visual data paths to accelerate the troubleshooting of connectivity problems.
- **Easy QoS:** Automates Quality of Service (QoS) to prioritize applications across your network.
- **EN Service Automation (ESA):** Automates deployment of physical and virtual network services.

Cisco NDP

Cisco Network Data Platform (NDP) is a new data collection and analytics subsystem, integrated directly into the software release of Cisco DNA Center (below), and will not be released as a separate product (Figure 22).

Note: All of the Cisco NDP software is included with the Cisco DNA Center appliance.

The NDP subsystem shares contextual analytics information with the Cisco ISE and NCP subsystems and provides this information back to the user (management layer).

Figure 22.   Cisco NDP (embedded within Cisco DNA Center)
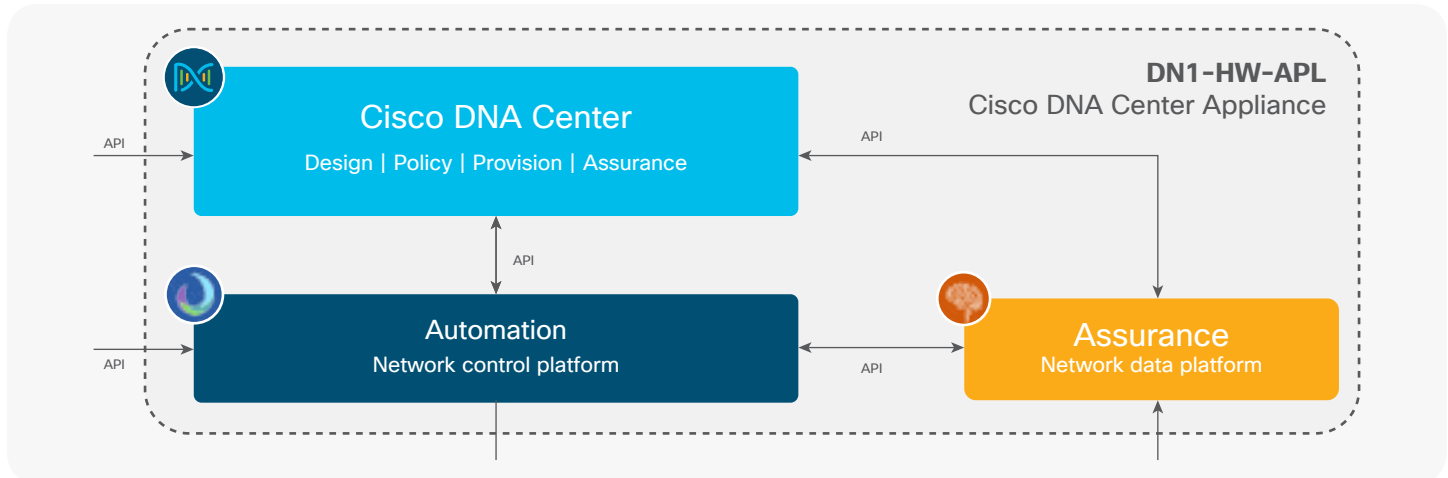
The basic role of NDP is to provide all of the data collection, analytics, and assurance services for the physical layer and network layer. NDP is capable of collecting multiple types of information from the network devices in a variety of forms, including syslog, SNMP, NetFlow, Switched Port Analyzer (SPAN), Streaming Telemetry, and others. NDP also collects and uses the contextual information shared from ISE and NCP (or partner systems such as Splunk, ServiceNow, etc.).

NDP then analyzes and correlates various network events across all of these different sources and learns about historical trends. It uses this information to provide contextual information back to NCP and ISE (and/or partner systems), and then provides network operational status and other information back to the management layer.

Note: Many of the NDP functions are available via published APIs. This enables external systems to interact with and/ or augment NDP. Refer to the partner ecosystem section for more information.

The various NDP services run as software packages (that can be added and upgraded independently), which share contextual data among themselves, with each processing specific functions within the overall subsystem. These services are then exposed to the management layer as various UI applications and/or workflows.

Cisco NDP is responsible for one primary service (app) in Cisco DNA Center 1.1:

- **Cisco DNA Assurance:** Provides the workflows and tools to visualize and apply network analytics to monitor and resolve issues in real time.

To read more about Cisco NDP, refer to the following link: https://www.cisco.com/c/en/us/solutions/collateral/ enterprise-networks/digital-network-architecture/datasheet-c78-738937.html.

Cisco ISE

Cisco Identity Services Engine (ISE) is a shipping product focused on general profiling, identity, and security policy compliance. ISE 2.3 is a new version that (in addition to new features and capabilities) includes important integration enhancements to interoperate with Cisco DNA Center.

Note: All of the Cisco ISE software is included with the Cisco ISE Secure Network Server (SNS) Series appliances.

The ISE subsystem integrates directly with the Cisco NCP and NDP subsystems (Cisco DNA Center) to provide contextual identity and policy information (Figure 23). This is done through various API-based data exchange mechanisms (REST and PxGrid), as well as automated certificate exchange for partner systems (for example, Cisco DNA Center). All of this information is then provided back to the user (management layer).

Figure 23. Cisco ISE (integrated with Cisco DNA Center via APIs)
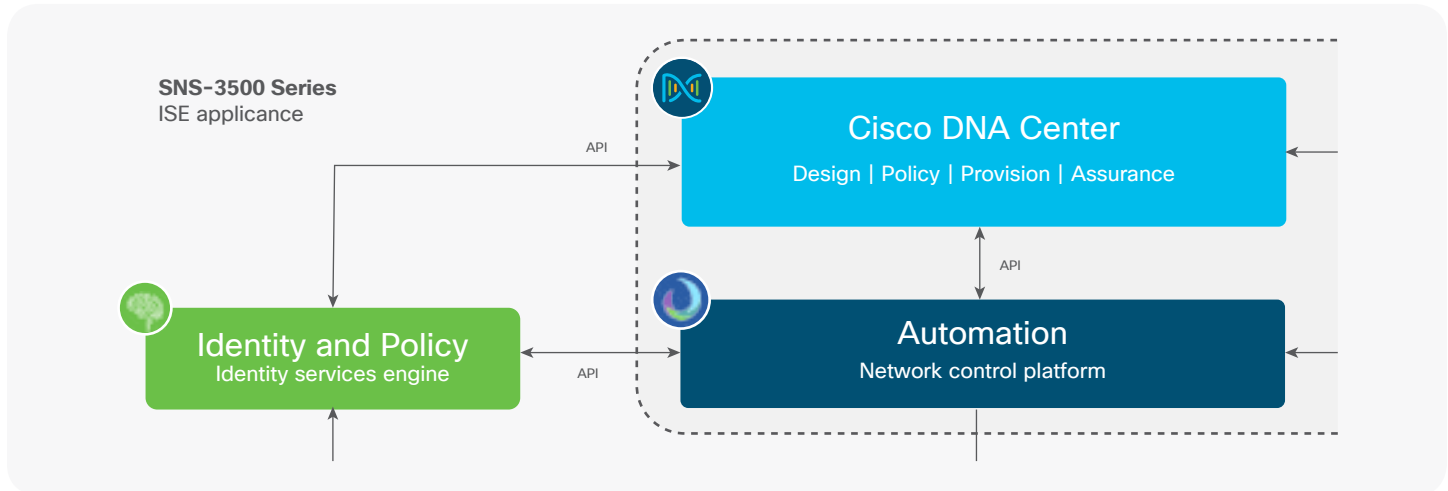
The basic role of ISE is to provide all of the identity and policy services for the physical layer and network layer. ISE is capable of identifying and profiling the network devices and endpoints in a variety of forms, including AAA/RADIUS, 802.1X, MAC Authentication Bypass (MAB), Web Authentication, EasyConnect, and others. ISE also collects and uses the contextual information shared from NDP and NCP (and/or partner systems, such as Active Directory, AWS, etc.).

ISE then places the profiled endpoints into the correct security group and host pool. It uses this information to provide information back to NCP and NDP, so the user (management layer) can create and manage group-based policies. ISE is also responsible for programming group-based policies on the network devices.

Note: Many of the ISE functions are available via published APIs. This enables external systems to interact with and/or augment ISE. Refer to the Partner Ecosystem section for more information.

Cisco ISE is responsible for one primary service (app) in Cisco DNA Center 1.0:

- **Cisco DNA Policy:** Provides the workflows and tools to manage virtual networks and security groups, and to create group-based policies and contracts.

To read more about Cisco ISE, refer to the following link(s):

https://www.cisco.com/c/en/us/products/security/identity-services-engine/

https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html.

Management layer

As noted earlier, users interact with the management layer of Cisco DNA Center. It is the user interface and user experience (UI/UX) layer, where all of the information about the other layers is exposed to the user. It is what provides the "intent-based networking" aspect of Cisco DNA.

A full understanding of the network layer (LISP, VXLAN, and Cisco TrustSec) or controller layer (Cisco NCP, NDP and ISE) 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 device and feature to create the consistent end-to-end behavior offered by SD-Access.

The management layer abstracts all of the complexities and dependencies of the other layers, and provides the user with a simple set of GUI tools and workflows to easily manage and operate the entire Cisco DNA network (hence the name Cisco DNA Center).

Cisco DNA Center provides two basic app types:

- **Cisco DNA Center settings:** Contains the controller settings, APIs, and tables to support communications between subsystems, as well as integrating partner services.
- **Cisco DNA Center applications:** Contains the workflow tools and contextual application data to support Cisco DNA user workflows (design, policy, provision, and assurance).

Cisco DNA Center settings are analogous to settings in other network management systems (for example, they configure role-based access [permissions], redundancy, backups, upgrades, etc.), but they also include specific tools and settings for integration between subsystems, as well as APIs to integrate with external (partner) systems.

Cisco DNA Center settings are visualized within the Settings page ✳ (Figure 24).

Figure 24.   System Settings page
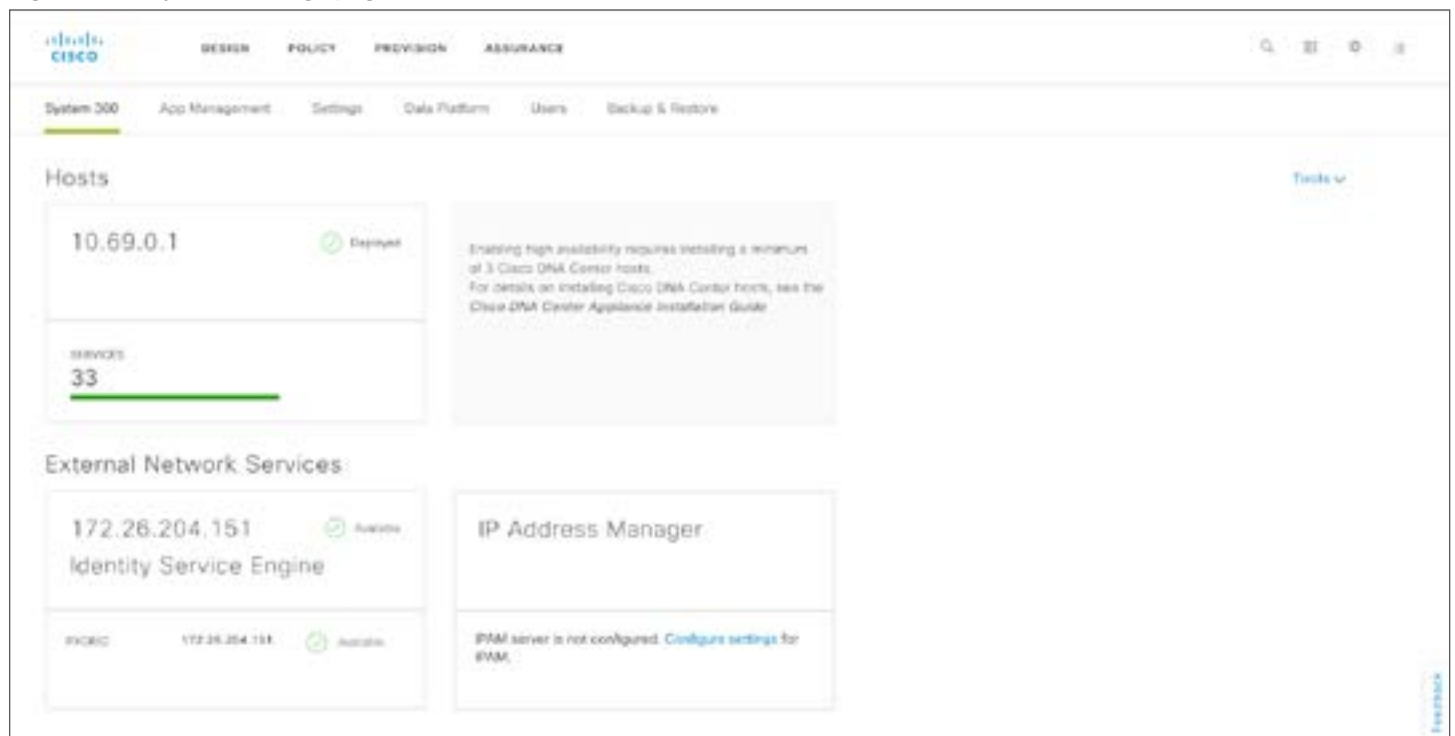
Cisco DNA Center applications are designed for user simplicity and are based on the primary workflows defined by Cisco DNA: **Design, Policy, Provision,** and **Assurance**.

Cisco DNA Center applications are visualized on the Apps page ⦙⦙⦙ (Figure 25).
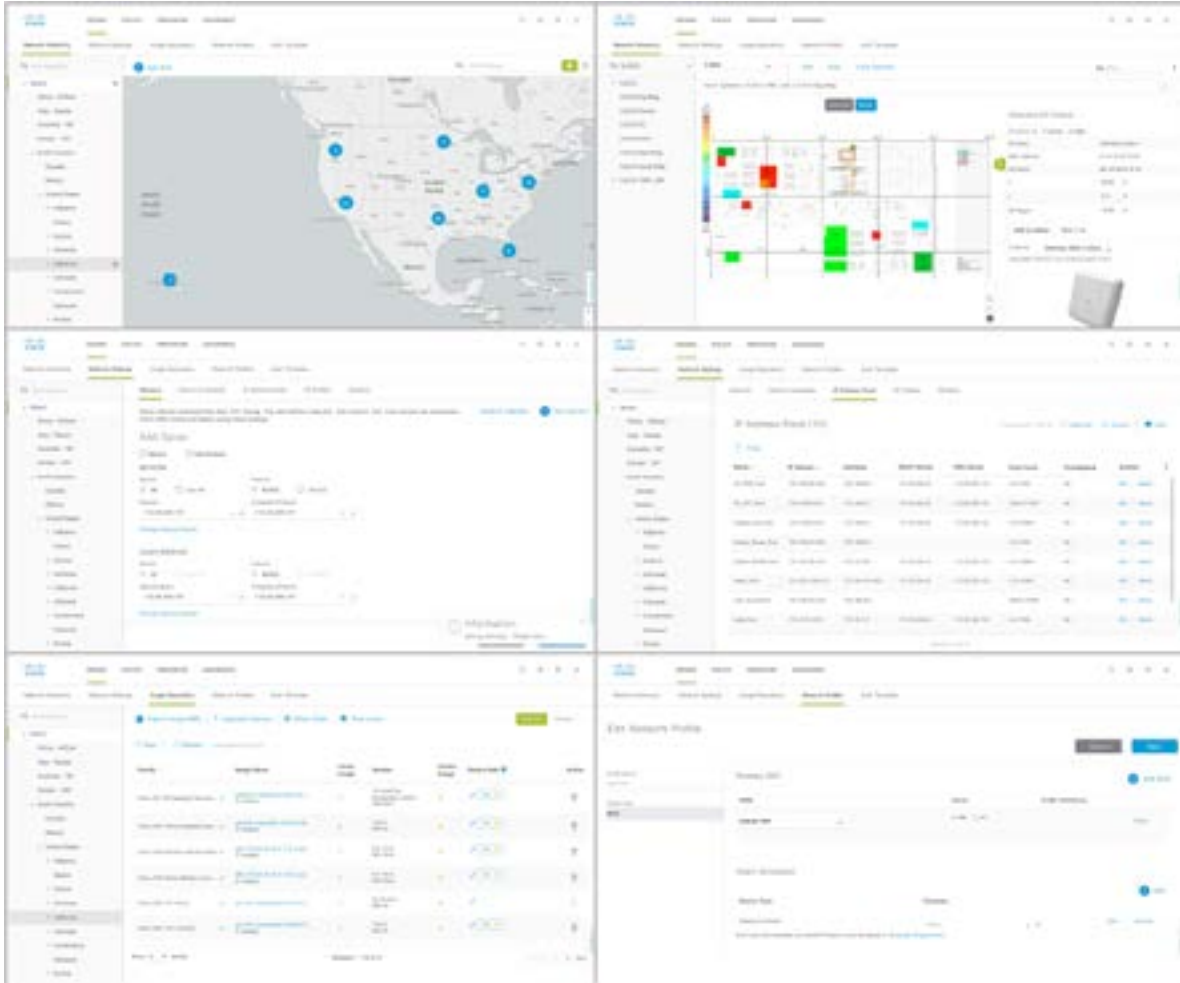
Figure 25. Cisco DNA Center Apps page
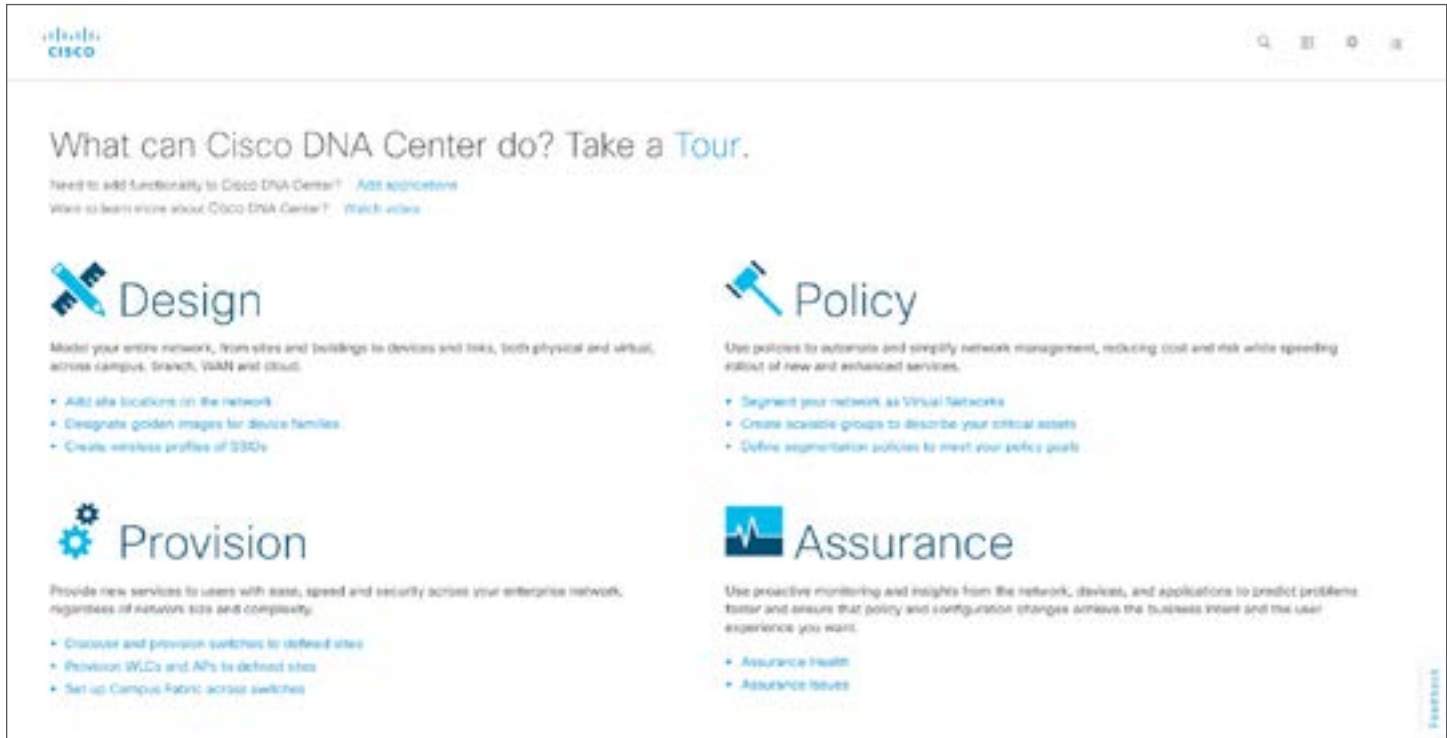
Cisco DNA Design

The Cisco DNA "design" workflow provides all of the tools to (logically) define your Cisco DNA network (Figure 26).

Here is a brief list of Cisco DNA design tools:

- **Network hierarchy:** Here is where you set up the geo location and building and floorplan details, and associate these with a unique site ID.
- **Network settings:** Here is where you set up network servers (such as DNS, DHCP, AAA, etc.), device credentials, IP management, and wireless settings.
- **Image management:** Here is where you manage the software images and/or maintenance updates, set version compliance, and download and deploy images.
- **Network profiles:** Here is where you define LAN, WAN, and WLAN connection profiles (such as SSID) and apply them to one or more sites.

Figure 26.   Cisco DNA design pages

The outcome of the design workflow is a hierarchical set of unique site IDs that define the global and forwarding configuration parameters of the various sites. The site IDs will be used by the provision workflow to deploy the Cisco SD-Access underlay and overlay networks.

Cisco DNA Policy

The Cisco DNA "policy" workflow provides all of the tools to (logically) define your Cisco DNA policies (Figure 27).

Here is a brief list of Cisco DNA policy tools:

- **Dashboard:** Here is where you monitor all of the VNs, security groups, policies, and recent changes.
- **Virtual Network:** Here is where you set up the virtual networks (or use Default_VN) and associate various security groups.
- **Policy Admin:** Here is where you define the access and/or traffic policies and contracts between source and destination security groups.
- **Contracts:** Here is where you define the applications (such as L4 Port) that should be enforced between source and destination security groups.
- **Registry:** Here is where you import security groups (e.g. from Cisco ISE) and/or create new (custom) security groups.

Figure 27.   Cisco DNA policy pages
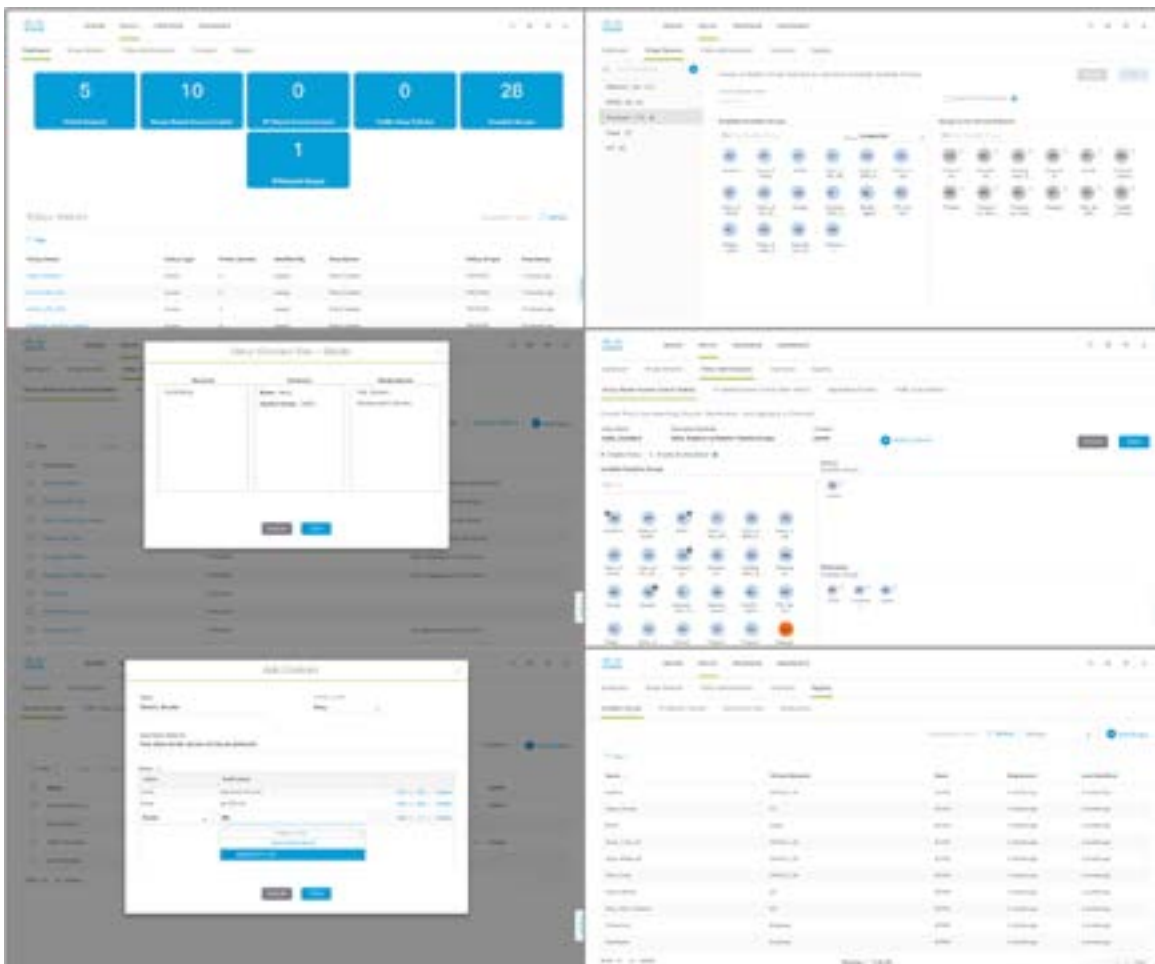
The outcome of the policy workflow is a set of virtual networks, security groups, and access and traffic policies that define the policy configuration parameters of the various sites. The VNs, groups, and policies will then be used by the provision workflow to deploy the Cisco SD-Access group-based policies.
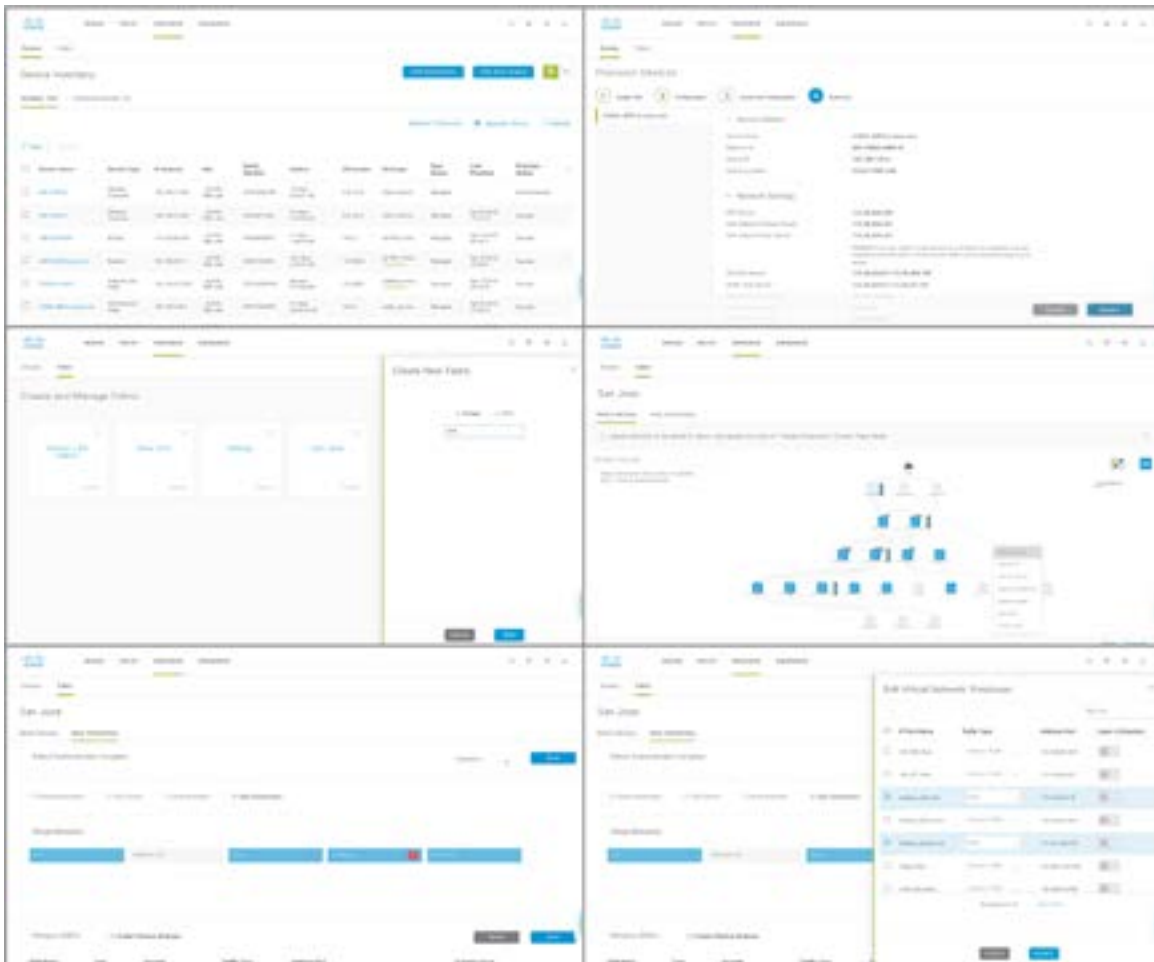
Cisco DNA Provision

The Cisco DNA "provision" workflow provides all of the tools to deploy your Cisco DNA network (Figure 28).

Here is a brief list of Cisco DNA provision tools:

- **Devices:** Here is where you assign devices to a site ID, confirm or update the software version, and provision the network underlay configurations.
- **Fabrics:** Here is where you set up the fabric domains (or use the default LAN fabric).
- **Fabric Devices:** Here is where you add devices to the fabric domain and specify device roles (e.g. control plane, border, edge, and WLC).
- **Host Onboarding:** Here is where you define the host authentication type (static or dynamic), and assign host pools (wired and wireless) to various VNs.

Figure 28.   Cisco DNA provision pages

The outcome of the provision workflow is the deployment of the network underlay, fabric overlay, and host onboarding configurations for various site IDs (from the design workflow), as well as access and traffic policies (from the policy workflow).

Cisco DNA Assurance

The Cisco DNA "assurance" workflow provides all of the tools to manage your Cisco DNA network (Figure 29).

Here is a brief list of Cisco DNA assurance tools:

- **Dashboard:** Here is where you monitor the global health of all (fabric and non-fabric) devices and clients, with scores based on the status of various sites.
- **Client 360:** Here is where you monitor and resolve client-specific status and issues (such as onboarding, app experience, etc.), with links to connected devices.
- **Devices 360:** Here is where you monitor and resolve device-specific status and issues (such as resource usage, loss and latency, etc.), with links to connected clients.
- **Issues and Trends:** Here is where you monitor and resolve open issues (reactive) and/or developing trends (proactive) with clients and devices at various sites.

Figure 29.   Cisco DNA assurance pages
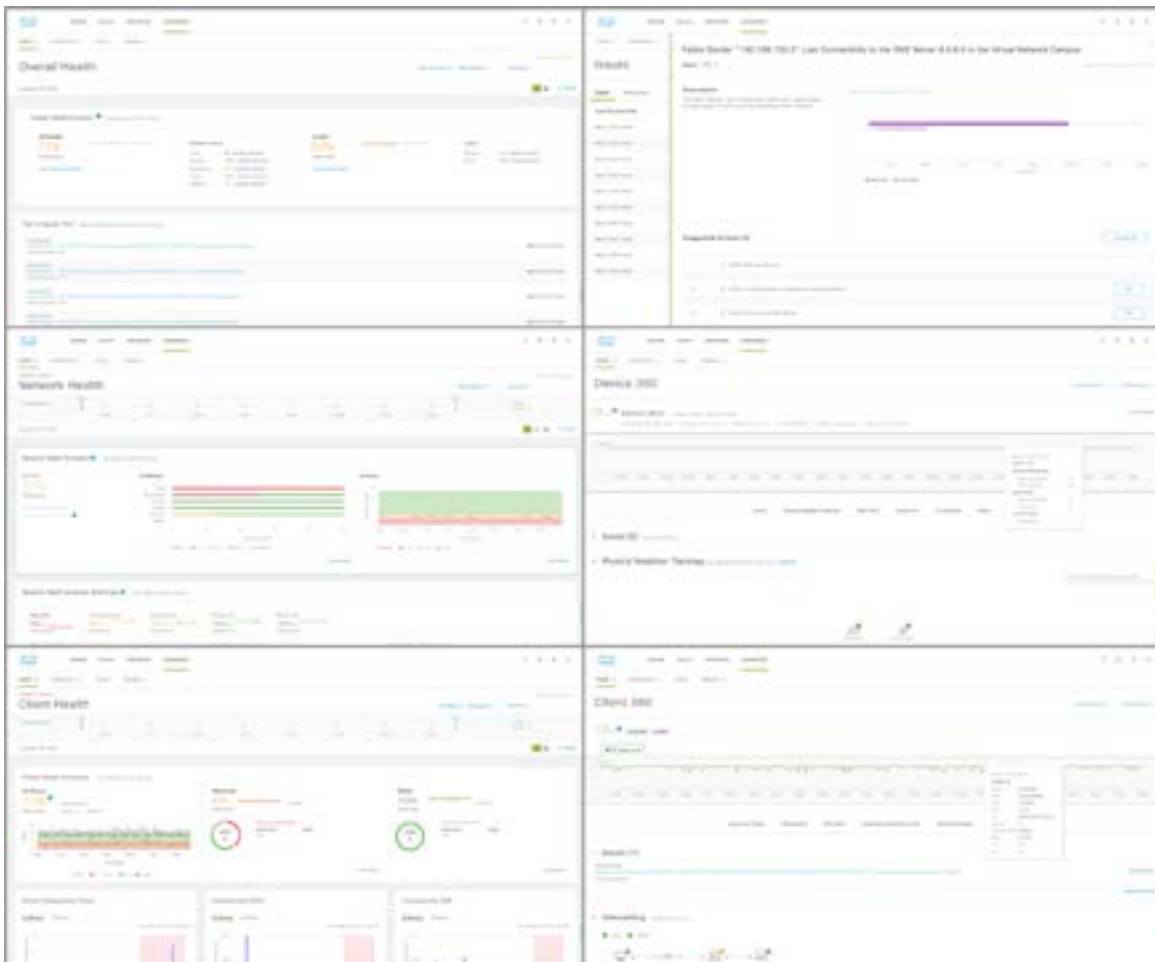
The assurance workflow is responsible for all operational management of the network underlay, fabric overlay, and host onboarding (from the design and provision workflows), as well as access and application policies (from the policy workflow).

To read more about Cisco DNA assurance, refer to the following link: https://www.cisco.com/c/en/us/solutions/enterprise-networks/dna-analytics-assurance.html.

Partner ecosystem

As part of the API-driven controller-based management framework and tools of Cisco DNA Center, we are able to provide direct solution-level access to established Cisco business partners, who can then integrate their own products with Cisco SD-Access as well as co-develop new and exciting capabilities.

While the list continues to grow, here are just a few examples:

- **Firewalls:** Share ID and policy attributes for group-based firewall rules.
- **DNS, DHCP, IPAM:** Share IP and name allocations for address pools.
- **Cloud:** Share ID, policy, and forwarding context for cloud-based apps.
- **NaaS and ETA:** Share ID and policy attributes to quarantine and mitigate threats.
- **VNFs:** Share ID, policy, and forwarding context for container-based apps.

To learn more about some of these, refer to the following link(s):

https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1862768

https://developer.cisco.com/site/sda/#key-integration-partners

There are many other exciting examples and possibilities. As the Cisco DNA partner ecosystem (led by Cisco DevNet) continues to grow and evolve, we will be adding many new ways to share and use contextual data between Cisco and our partners.

DevNet

Cisco DevNet will help you learn all you need to know to work with the APIs in the Cisco Digital Network Architecture. Explore programming foundations and APIs. Learn about Cisco DNA Center, as well as device-level APIs provided by YANG data models such as NETCONF and RESTCONF.

https://developer.cisco.com/site/dna/

https://learninglabs.cisco.com/tracks/programming-dna/

Conclusion

Now you have a good understanding of the entire **Cisco SD-Access 1.0** solution, at medium technical level, and you should be able to describe all of the 5 main layers (physical, network, controller, management and partner), their basic role in SD-Access, their sub-layers, and how they relate to one another.

This will enable you to begin designing your future Cisco enterprise network and provide a solid foundation to continue your studies. We encourage you to visit the various reference links provided throughout the document, and to try out Cisco SD-Access for yourself.

Cisco SD-Access marks a completely new era in enterprise networking. With this document, you are taking your first steps into the future.

References

Here are some other useful references for Cisco DNA and SD-Access:

- Cisco.com/go/sdaccess
- Cisco.com – Software-Defined Access Solution Overview

- Cisco.com – Software-Defined Access Solution FAQ
- Cisco.com – Software-Defined Access Migration Guide

- Cisco.com/go/dnacenter
- Cisco.com – Cisco DNA Ready Infrastructure Guide
- Cisco.com – Cisco Digital Network Architecture Vision White Paper

- TechWiseTV – Introduction to Cisco Software-Defined Access
- TechWiseTV – A Deeper Look at Cisco Software-Defined Access

Glossary

Table 8 provides some basic definitions for acronyms and/or terminology used in this document.

Table 8. Glossary

Acronym/term	Definition/description
AAA	Authentication, authorization, and accounting
ACL	Access control list
AP	Access point
API	Application programming interface
BGP	Border Gateway Protocol
CAPWAP	Control and Provisioning of Wireless Access Points
DHCP	Dynamic Host Configuration Protocol
Cisco DNA	Cisco Digital Network Architecture
EID	Endpoint identifier (LISP)
ETA	Encrypted Threat Analytics
IGP	Interior Gateway Protocol (EIGRP, OSPF, IS-IS)
IPAM	IP address management
ISE	Identity Services Engine
L2	Layer 2 (switching – Data Link Layer of the OSI model)
L3	Layer 3 (routing – Network Layer of the OSI model)

Acronym/term	Definition/description
LAN	Local Area Network
LISP	Locator/Identity Separation Protocol
MTU	Maximum Transmission Unit
NaaS	Network as a Sensor
NCP	Network Control Platform
NDP	Network Data Platform
RLOC	Routing locator (LISP)
SD-Access	Software-Defined Access
SGT	Scalable Group Tag (or security group tag)
SGACL	Security Group ACL
STP	Spanning Tree Protocol
SXP	SGT Exchange Protocol
VLAN	Virtual LAN
VXLAN	Virtual Extensible LAN
VN	Virtual Network (VRF)
VNF	Virtual Network Function
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network