Cisco Software-Defined Access

Enabling Intent-based Networking
# Table of contents

**Preface**

- Authors
- Acknowledgments
- Organization of this book
- Intended Audience
- Book Writing Methodology

**Introduction**

- Executive Summary
- The Network Evolution

**SD-Access Overview**

- Software-Defined Access Overview
- SD-Access Benefits

**SD-Access Fabric**

- Fabric Components
- Fabric Operation
- Fabric Considerations
- Fabric Deployment Models
- External Connectivity
- Fabric Packet Walks
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA Center</td>
<td>94</td>
</tr>
<tr>
<td>DNA Center Overview</td>
<td>95</td>
</tr>
<tr>
<td>SD-Access Policy</td>
<td>98</td>
</tr>
<tr>
<td>Policy and Services Overview</td>
<td>99</td>
</tr>
<tr>
<td>Policy Architecture</td>
<td>106</td>
</tr>
<tr>
<td>Policy Benefits</td>
<td>109</td>
</tr>
<tr>
<td>Policy in Action</td>
<td>112</td>
</tr>
<tr>
<td>SD-Access Automation</td>
<td>114</td>
</tr>
<tr>
<td>Automation and Orchestration in DNA Center</td>
<td>115</td>
</tr>
<tr>
<td>Automating SD-Access with DNA Center</td>
<td>118</td>
</tr>
<tr>
<td>SD-Access Assurance</td>
<td>123</td>
</tr>
<tr>
<td>Assurance</td>
<td>124</td>
</tr>
<tr>
<td>Telemetry</td>
<td>126</td>
</tr>
<tr>
<td>Health and Insights</td>
<td>128</td>
</tr>
<tr>
<td>Reporting</td>
<td>134</td>
</tr>
<tr>
<td>Integration with Partner Ecosystems</td>
<td>135</td>
</tr>
<tr>
<td>Introduction</td>
<td>136</td>
</tr>
<tr>
<td>APIs &amp; Programmability</td>
<td>137</td>
</tr>
<tr>
<td>Ecosystem Integrations</td>
<td>139</td>
</tr>
</tbody>
</table>
Summary, Next Steps, and References 142

Summary 143
Next Steps 145
References 147
Acronyms 148
Cisco Software-Defined Access
Enabling Intent-based Networking
Preface
Authors

This book represents a collaborative effort between Technical Marketing, Product Management, Advanced Services, Engineering, and Sales Engineers during a week-long intensive session at Cisco Headquarters in San Jose, CA.

- Craig Hill – Systems Engineering
- Darrin Miller – Technical Marketing
- Dave Zacks – Technical Marketing
- Josh Suhr – Advanced Services
- Karthik Kumar Thatikonda – Technical Marketing
- Kedar Karmarkar – Technical Marketing
- Sanjay Hooda – Engineering
- Satish Kondalam – Technical Marketing
- Saurav Prasad – Technical Marketing
- Shawn Wargo – Technical Marketing
- Simone Arena – Technical Marketing
- Vaibhav Katkade – Product Management
- Vikram Pendharkar – Product Management
Acknowledgments

A special thanks to Cisco’s Enterprise Networking Business Product Management, Engineering, Sales and Services teams who supported the realization of this book. We would also like to thank Cynthia Resendez for her exceptional resource organization and support throughout our journey, and Sehjung Hah for making sure that everything worked smoothly and that all thirteen authors made it to the end.

We are also genuinely appreciative to our Book Sprints (www.booksprints.net) team:

- Adam Hyde (Founder)
- Barbara Ruhling (CEO)
- Henrik van Leeuwen (Illustrator)
- Juan Carlos Gutiérrez Barquero (Technical Support)
- Julien Taquet (Book Producer)
- Laia Ros (Facilitator)
- Raewyn Whyte (Proofreader)

Laia and the team created an enabling environment that allowed us to exercise our collaborative and technical skills to produce this technical publication to meet a growing demand.

Thanks to Carl Solder, Rohan Grover, Victor Moreno, Muninder Sambi, Shyam Maniyan, Dan Kent, Yi Xue, Ronnie Ray, Bipin Kapoor, Kevin Skahill, Ziad Sarieddine, Jeff McLaughlin, Nicolas Coulet, Ramit Kanda, and Sehjung Hah for supporting this effort.
Organization of this book

This book is intended to be read sequentially. While each chapter could be reviewed in any order, the concepts discussed in the book build sequentially, so the reader is recommended to review the topics in the order presented.

The topics that the book covers include an introduction to SD-Access, discussing the business drivers for enterprises, and the challenges to enterprise IT to enable those business outcomes today. Next, we examine an overview of SD-Access, providing a synopsis of the SD-Access solution and discussing how SD-Access overcomes some of the challenges that cannot be solved with existing network tools and techniques. Following this, we dive deep into the technology behind SD-Access, including components, operation, and deployment options. We then examine the automation and orchestration framework that drives the SD-Access workflows – DNA Center. Areas including policy, automation, and assurance are discussed in detail. Finally, we explore the integration with partner ecosystems and wrap up with a summary and a review of recommended next steps.
Intended Audience

Network and IT professionals are always looking for ways to improve the design and operations of their networks. This book focuses on the SD-Access based network architecture for wired-wireless integration with WAN, DC, and services. While the network architects and administrators will reap maximum benefits from this book, the IT professionals will be able to utilize the book to understand the new networking technologies and concepts in their network environments and how it simplifies things for them. Security architects can also utilize the book to understand how the new SD-Access architecture can help them extend the security perimeter in their enterprise networks to the edge.

The elements in this book cover fabric technologies, policy, automation, assurance and how these technologies can be utilized by network professionals to help the security and simplification of IT deployments.
Simplicity has been an overriding theme in designing SD-Access. The idea of the book is to present readers with the current challenges in enterprise networking, where the existing networking technologies are lacking, and the underpinnings of SD-Access that solve these challenges for NetOps and SecOps teams without losing sight of simplicity.

A group of thirteen Cisco Engineers from diverse backgrounds accepted the challenge of writing a book that changes the paradigm of enterprise networking. At the end of day one, the task seemed even more daunting, given the breadth of areas that SD-Access covers in an enterprise network. However the team persisted, and after hundreds of hours of diligent penmanship, this book was born! The Book Sprints (www.booksprints.net) methodology captured each of our unique strengths, fostered a team-oriented environment, and accelerated the overall time to completion.

#HardtoTalkaboutSimplicity
Introduction
Executive Summary

Digital transformation is creating new opportunities in every industry. In healthcare, doctors are now able to monitor patients remotely and leverage medical analytics to predict health issues. In education, technology is enabling a connected campus and a more personalized, equal access to learning resources. In retail, shops are able to provide an omnichannel experience by being able to engage online and in-store, with location awareness. In today’s world, digital transformation is absolutely necessary for businesses to stay relevant!

For any organization to successfully transition to a digital world, they must invest in their network. It’s the network that connects all things and is the cornerstone where digital success is realized or lost. It is the pathway for productivity and collaboration and an enabler of improved end-user experience. It is also the first line of defense to securing enterprise assets and intellectual property.

Software-Defined Access is the industry’s first intent-based networking solution for the enterprise. An intent-based network treats the network as a single system that provides the translation and validation of the business intent (or goals) into the network and returns actionable insights.

DIAGRAM  Intent-based Network for a Digital Business
SD-Access provides automated end-to-end services (such as segmentation, quality of service, analytics, and so on) for user, device, and application traffic. SD-Access automates user policy so organizations can ensure the appropriate access control and application experience are set for any user or device to any application across the network. This is accomplished with a single network fabric across LAN and WLAN which creates a consistent user experience, anywhere, without compromising on security.

**SD-Access Benefits**

- **Automation**: Consistent management of wired and wireless network provisioning and policy.
- **Policy**: Automated network segmentation and group-based policy.
- **Assurance**: Contextual insights for fast issue resolution and capacity planning.
- **Integration**: Open and programmable interfaces for integration with third-party solutions.
The Network Evolution

Today's networks support a very different IT environment compared to just a few years ago. There has been a significant rise in the use of mobile clients, increased adoption of cloud-based applications, and the introduction of the Internet of Things (IoT).

As businesses have digitized, the scale of networks and networking needs have grown over the years, without a proportionate increase in IT resources. The end-user expectations have also been rising, with businesses continually expecting IT to keep up with their evolving technology and growth needs.

The networking technologies that have been the foundation of providing interconnectivity between clients, devices, and applications have remained fairly static. While today's IT teams have a number of technology choices to design and operate their networks, there hasn’t been a comprehensive, turnkey solution to address their evolving enterprise needs around mobility, IoT, cloud, and security.

In this section, we’ll explore several broad areas of modern networking challenges in the context of a number of common use cases:

**Network Deployment**

- Implementation complexity
- Wireless considerations

**Service Deployment**

- Network segmentation
- Access control policies
- User & device onboarding
Network Operations

- Slow issue resolution.

Network Deployment

Implementation Complexity

Over time, network operators must accommodate new network services by implementing new features and design approaches but do so on top of a traditional network infrastructure. In addition, the network must continually be optimized for high availability, new applications, etc., resulting in "snowflake" networks – no two are alike. While this may meet functional goals, this also makes the networks complex to understand, troubleshoot, predict, and upgrade.

A slow-to-deploy network impedes the ability of many organizations to innovate rapidly and adopt new technologies such as video, collaboration, and connected workspaces. The ability of a company to adopt any of these is impeded if the network is slow to change and adapt. It is difficult to automate the many, many potential variations of "snowflake" network designs and this limits the ability to adopt automation in today's networks to drive greater operational efficiencies for an organization.

---

The bottom line

Too many network variations and combinations (snowflakes) make it challenging to adopt new capabilities and services.

---

Wireless Considerations

In addition, one of the major challenges with wireless deployment today is that it does not easily utilize network segmentation. While wireless can leverage multiple SSIDs for traffic separation over-the-air, these are limited in the number that can be deployed and are ultimately mapped back into VLANs at the WLC. The WLC itself has no concept
of VRF / Layer 3 segmentation, making deployment of a true wired and wireless network virtualization solution very challenging.

**The Bottom Line**

Traditional wireless networks are managed separately and difficult to segment.

**Service Deployment**

**Network Segmentation**

Let’s look at some of the options available today and their challenges for creating network segmentation.

**VLANs**

The simplest form of network segmentation relies on VLANs. You may not be used to thinking about a VLAN as network segmentation technology, but that is what a VLAN is: a segmented Layer 2 domain. By placing users and devices in different VLANs, we are able to enforce traffic controls between them at the Layer 3 boundary. For wireless, different SSIDs might be used for separation into the air, but then these are mapped into VLANs on the wired side.

The challenge with VLANs as a segmentation method is two-fold: their span and the topology-related issues they bring along with them. In terms of span, most organizations choose to constrain VLANs to a relatively small area (often limited to one wiring closet). Because of this, many organizations end up managing hundreds or even thousands of VLANs in a typical deployment, making IP address planning much more complex to deploy and manage.

Key challenges with using VLANs include the following:

- A widely-spanned VLAN is vulnerable to Layer 2 loops in redundant network designs.
- Large Layer 2 designs are very inefficient (50% of ports blocking typically).
- Large Layer 2 designs are at risk of meltdowns if an uncontrolled Layer 2 loop should occur for any reason.
Traffic filtering options for intra-VLAN traffic are also typically much more limited than those available at a Layer 3 boundary.

**the bottom line**

VLANs are simple but, in this case, simple is not best – a flat Layer 2 design exposes the organization to too many potential events that could take down the network, and in addition, managing hundreds of VLANs is daunting for most organizations.

**VRFs with VRF-Lite**

Another approach – one that leverages Layer 3 – is to segment the network by using VRFs (Virtual Routing and Forwarding instances – essentially, separate versions of the IP routing table). This has the benefit that segmentation can be provided without the need to build large, complex ACLs to control traffic flows – since traffic between different VRFs can only flow as the network manager dictates via the network topology (typically, via route leaking or through a firewall).

Challenges with the VRF-Lite approach are as follows:

- VRF-Lite using 802.1q trunks between devices is relatively simple to implement on a few devices but becomes very cumbersome very quickly when implemented more widely.
- VRF-Lite requires separate routing protocol processes per VRF, resulting in increased CPU load and complexity.
- The typical rule-of-thumb is that VRF-Lite deployments should not be scaled beyond 8–10 VRFs total, as they become far too unwieldy to manage end-to-end in an enterprise deployment at a larger scale.

**VRFs with MPLS VPNs**

The alternative, MPLS VPNs, have a steep learning curve since they require the network manager to become familiar with many new MPLS-specific capabilities, including LDP for label distribution, and Multi-Protocol BGP as a control plane. Moreover, they need to understand how to debug MPLS-enabled networks when issues arise.
Challenges with MPLS VPNs are as follows:

- MPLS VPNs will scale much better than VRF-Lite; they are often too complex for many network managers to tackle, especially across an end-to-end network deployment.
- MPLS VPN support is not available pervasively across all network platforms.

**The bottom line**

Despite having VRF capabilities for more than ten years, only a small percentage of organizations have deployed VRF segmentation in any form. Why? In a word – complexity.

**Network Policies**

Policy is one of those abstract words that can mean many different things to many different people. However, in the context of networking, every organization has multiple policies that they implement. Use of security ACLs on a switch, or security rule-sets on a firewall, is security policy. Using QoS to sort traffic into different classes, and queues to prioritize one application versus another is a QoS policy. Placing devices into separate VLANs based on their role is a device-level access control policy.

Today’s network manager typically uses a few sets of common policy tools every day: VLANs, subnets, and ACLs. For example:

- Adding voice to a network? This implies carving a new set of voice VLANs and associated subnets.
- Adding IP cameras and streaming video endpoints? More VLANs and subnets again.

This is why an enterprise network today ends up with hundreds, or even thousands, of VLANs and subnets. The level of complexity in designing and maintaining this is obvious in and of itself – and yet it also requires the further maintenance of many DHCP scopes,
IPAM tools, and the complexity associated with managing a large IP address space across all of these various VLANs and functions.

Today’s network, faced with many internal and external threats, also needs to be secure. This makes it necessary to create and implement – and maintain on an ongoing basis – large Access Control Lists, implemented on network devices including switches, routers, and firewalls, most often at Layer 3 boundaries in the network deployment.

**The bottom line**

The traditional methods used today for policy administration (large and complex ACLs on devices and firewalls) are very difficult to implement and maintain.

**User & Device Onboarding**

No matter which solution is chosen today – a Layer 2 or Layer 3 network design, a segmented or non-segmented network approach – there is always the issue of the optimal approach to onboard users and devices into the network.

This could be as simple as hard-coding a VLAN/subnet to a wired port or wireless SSID, but there are some common challenges:

- While functional, this offers little real security, since anyone connecting into that port or SSID is associated with that “role” in the network.
- Either on the first-hop switch, or on a firewall ten hops away, that user’s IP address will be examined and the appropriate security policy will be controlled and enforced. Essentially, the IP address ends up being used as a proxy for identity. However, this is hard to scale, and to manage.

Otherwise, a VLAN/subnet could be assigned dynamically using 802.1x or another authentication method but there are some common challenges:

- While the use of 802.1x is common in wireless deployments, it is less common in wired network use.
Many issues exist as deployment blockers, such as 802.1x supplicant settings on the device, 802.1x support on the device, switching VLANs/subnets dynamically based on roles, 802.1x support and features on the network equipment, and so on.

And once that user/device identity is established, how can it be carried end-to-end within the network today? There is no place within an IP packet header to carry this user/device mapping. So, once again, IP addresses are used as a proxy for this. However, this leads to a proliferation of user/device subnets, and all of the attendant complexity that goes along with this.

---

**The Bottom Line**

Most organizations want to establish user/device identity and use it end-to-end for policy. However, many find this to be a daunting task.

---

**Network Operations**

**Slow Issue Resolution**

Many networks today provide very limited visibility into network operation and use. The wide variety of available network monitoring methods – SNMP, Netflow, screen scraping, and the like – and the mixture of availability of these tools across various platforms, makes it very difficult to provide comprehensive, end-to-end insights derived from ongoing monitoring in today's network deployments.

Without insight into ongoing operational status, organizations often find themselves reacting to network problems, rather than addressing them proactively – whether these problems are caused by issues or outages, or simply brought on by growth or changes in user/application patterns.

Many organizations would place significant value on being able to be more knowledgeable about how their network is being used, and more proactive in terms of network visibility and monitoring. A more comprehensive, end-to-end approach is
needed – one that allows insights to be drawn from the mass of data that potentially can be reported from the underlying infrastructure.

**the bottom line**
Most organizations lack comprehensive visibility into network operation and use – limiting their ability to proactively respond to changes.

**Tying It All Together**

So, what does it take to roll out networks and the associated policies end-to-end today?

First, the network manager has to settle on a given network design: multi-layer access, routed access, access virtualized using VRF-Lite or MPLS VPNs, etc. There are many considerations and tradeoffs associated with this today, so this is not necessarily a simple choice.
Based on the diagram above, the following steps represent a typical service deployment:

1. Map to user groups in Active Directory or a similar database for user authentication.
2. Link these AD identities to the AAA server (such as ISE) if using dynamic authentication. This provides each identity with an appropriate corresponding VLAN/subnet.
3. Define and carve out new VLANs and associated subnets for the new services to be offered. Then, implement these VLANs and subnets on all necessary devices (switches, routers, and WLCs).
4. Secure those subnets with the appropriate device or firewall ACLs, or network segmentation. If using a segmented, virtualized network approach, extend these VRFs end-to-end using VRF-Lite or MPLS VPNs.
5. To do all of this, it is necessary to work across multiple user interfaces – the AD GUI, the AAA GUI, the WLC GUI for wireless; the switch or router CLI for wired – and stitch together all of the necessary constructs manually.

And when it becomes necessary to implement another group of users or devices or to alter a policy associated with them, all of these steps must be repeated all over again.

---

No wonder it takes days or weeks to roll out new network services today!
SD-Access Overview
Software-Defined Access Overview

Cisco's Software-Defined Access (or SD-Access) solution is a programmable network architecture that provides software-based policy and segmentation from the edge of the network to the applications. SD-Access is implemented via Cisco Digital Network Architecture Center (DNA Center) which provides design settings, policy definition and automated provisioning of the network elements, as well as assurance analytics for an intelligent wired and wireless network.

In an enterprise architecture, the network may span multiple locations (or sites) such as a main campus, remote branches, and so on, each with multiple devices, services, and policies. The Cisco SD-Access solution offers an end-to-end architecture that ensures consistency in terms of connectivity, segmentation, and policy across different locations (sites).

These can be described as two main layers:

- **SD-Access Fabric**: the physical and logical network forwarding infrastructure.
- **DNA Center**: the automation, policy, assurance and integration infrastructure.
This chapter will outline each of the major SD-Access solution components, with additional details in following chapters.

**SD-Access Fabric**

As described earlier, part of the complexity in today's network comes from the fact that policies are tied to network constructs such as IP addresses, VLANs, ACLs, etc.

What if the enterprise network could be divided into two different layers, for different objectives? One layer dedicated to the physical devices and forwarding of traffic (known as an **underlay**), and another entirely virtual layer (known as an **overlay**), where wired and wireless users and devices are logically connected together, and services and policies are applied.
This provides a clear separation of responsibilities and maximizes the capabilities of each sublayer. This approach would dramatically simplify deployment and operations because a change of policy would only affect the overlay, and the underlay would not be touched.

The combination of an underlay and an overlay is called a "network fabric."

The concepts of overlay and fabric are not new in the networking industry. Existing technologies such as MPLS, GRE, LISP, OTV, etc. are all examples of network tunneling technologies which implement an overlay. Another common example is Cisco Unified Wireless Network (CUWN), which uses CAPWAP to create an overlay network for wireless clients.

So, what is unique about the SD-Access Fabric? Let's start by defining the key SD-Access components.
SD-Access Network Underlay

The SD-Access network underlay (or simply: underlay) is comprised of the physical network devices, such as routers, switches, and wireless LAN controllers (WLCs) plus a traditional Layer 3 routing protocol. This provides a simple, scalable and resilient foundation for communication between the network devices. The network underlay is not used for client traffic (client traffic uses the fabric overlay).

All network elements of the underlay must establish IP connectivity between each other. This means an existing IP network can be leveraged as the network underlay. Although any topology and routing protocol could be used in the underlay, the implementation of a well-designed Layer 3 access topology is highly recommended to ensure consistent performance, scalability, and high availability.

This eliminates the need for STP, VTP, HSRP, VRRP, etc. In addition, running a logical fabric topology on top of a prescriptive network underlay provides built-in functionality for multi-pathing, optimized convergence, and so on, and simplifies the deployment, troubleshooting, and management of the network.

DNA Center provides a prescriptive LAN automation service to automatically discover, provision, and deploy network devices according to Cisco Validated Design best practices. Once discovered, the automated underlay provisioning leverages Plug and Play (PnP) to apply the required protocol and IP address configurations.

The DNA Center LAN Automation uses a best practice IS-IS routed access design. The main reasons for IS-IS are:

- IS-IS is protocol agnostic, so it works with IPv4 and IPv6 addresses
- IS-IS can work with only Loopback interfaces, and doesn’t require an address on each L3 link
- IS-IS supports an extensible TLV format for emerging use cases.
**SD-Access Fabric Overlay**

The SD-Access fabric overlay (or simply: overlay) is the logical, virtualized topology built on top of the physical underlay. As described earlier, this requires several additional technologies to operate.

SD-Access fabric overlay has 3 main building blocks:

- **Fabric data plane**: the logical overlay is created by packet encapsulation using Virtual Extensible LAN (VXLAN), with Group Policy Option (GPO).
- **Fabric control plane**: the logical mapping and resolving of users and devices (associated with VXLAN tunnel endpoints) is performed by Locator/ID Separation Protocol (LISP).
- **Fabric policy plane**: where the business intent is translated into a network policy, using address-agnostic Scalable Group Tags (SGT) and group-based policies.

VXLAN-GPO 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 group-based policy (SGT).

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.

**SD-Access Policy**

A fundamental benefit of SD-Access is the ability to instantiate logical network policy, based on services offered by the fabric. Some examples of services that the solution offers are the following:

- Security segmentation services
- Quality of Service (QoS)
- Capture/Copy services
• Application visibility services

These services are offered across the entire fabric independently of device-specific address or location.

**SD-Access Segmentation**

Segmentation is a method or technology used to separate specific groups of users or devices from other groups for the purpose of security, overlapping IP subnets, etc. In SD-Access fabric, VXLAN data-plane encapsulation provides network segmentation by using the VNI (Virtual Network Identifier) and Scalable Group Tag (SGT) fields in its header.

SD-Access fabric provides a simple way to implement hierarchical network segmentation: macro segmentation and micro segmentation.

**Macro segmentation:** logically separating a network topology into smaller virtual networks, using a unique network identifier and separate forwarding tables. This is instantiated as a virtual routing & forwarding (VRF) instance and referred to as a Virtual Network.

A **Virtual Network** (VN) is a logical network instance within the SD-Access fabric, providing Layer 2 or Layer 3 services and defining a Layer 3 routing domain. The VXLAN VNI is used to provide both the Layer 2 and Layer 3 Segmentation.

**Micro segmentation:** logically separating user or device groups within a VN, by enforcing source to destination access control permissions. This is commonly instantiated using access control lists (ACL), also known as an access control policy.

A **Scalable Group** is a logical object ID assigned to a “group” of users and/or devices in the SD-Access fabric, and used as the source and destination classifier in Scalable Group ACLs (SGACLs). The SGT is used to provide address-agnostic group-based policies.
SD-Access Fabric Wireless

Administrators may notice that a traditional Cisco Unified Wireless Network (CUWN) design provides some of the same advantages of SD-Access. For example, here are some of the common attributes:

- Tunneled overlay network (via CAPWAP enscapsulation and separate control-plane)
- Some levels of infrastructure automation (e.g. AP management, configuration management, etc.)
- Simple wireless user or device mobility (also known as client roaming).
- Centralized management controller (WLC).

But the CUWN approach comes with some tradeoffs:

- Only wireless users can benefit from the CAPWAP overlay, and does not apply to wired users.
- Wireless traffic must be tunneled to a centralized anchor point, which may not be optimal for many applications.

In addition, there are several advantages unique to wired users:

- Wired users can benefit from the performance and scalability that a distributed switching data plane provides.
- Wired users also benefit from advanced QoS and innovative services such as Encrypted Traffic Analytics (ETA), available in the switching infrastructure.

In other words, each domain (wired and wireless), has different advantages. So, what is unique about the SD-Access wireless?

SD-Access fabric provides the best of the distributed wired and centralized wireless architectures by providing a common overlay and extending the benefits to both wired and wireless users. Finally, with SD-Access fabric, customers can have a common policy and one unified experience for all their users independently of the access media.
**SD-Access Management with DNA Center**

The Cisco DNA Center provides the central management plane for building and operating a SD-Access Fabric. The management plane is responsible for forwarding configuration and policy distribution, as well as device management and analytics.

There are two main functions of DNA Center: automation and assurance.

DNA Center automation provides the definition and management of SD-Access group-based policies, along with the automation of all policy-related configurations. DNA Center integrates directly with Cisco ISE to provide host onboarding and policy enforcement capabilities.

**Automation & Orchestration**

Automation can be generally defined as a technology or system that performs an action or task without human assistance. A single task may require multiple actions but will have a single expected outcome. Orchestration is automating the execution of an overall workflow or process and may require multiple related tasks and involve multiple systems.

This is the basis on which the industry terminology "Software-Defined" can be applied to the automation and orchestration of Enterprise Campus "Access" network environments, as well as translate the user "intent" into meaningful configuration and verification tasks.

So, how are these applied to SD-Access? Cisco DNA uses controller-based automation as the primary configuration and orchestration model, to design, deploy, verify, and optimize wired and wireless network components for both non-fabric and fabric-based deployments.

With DNA Center completely managing the infrastructure, IT teams can now operate on an abstracted intent-based layer and not have to worry about the implementation details. This results in simplifying operations for the IT teams by minimizing the chances of making a human error and more easily standardizing the overall network design.
Network Assurance

Network Assurance quantifies availability and risk from an IT network perspective, based on a comprehensive set of network analytics. Beyond general network management, network assurance measures the impact of network change on security, availability, and compliance.

DNA Center Assurance was developed as a full management and operations solution to address the most common customer challenges. Cisco DNA Center provides multiple forms and levels of assurance and analytics, for both non-fabric and fabric-based components.

The key enabler to DNA Assurance is the analytics piece: the ability to continually collect data from the network and transform it into actionable insights. To achieve this, DNA Center collects a variety of network telemetry, in traditional forms (e.g. SNMP, Netflow, syslogs, etc) and also emerging forms (NETCONG/YANG, streaming telemetry, etc. DNA Assurance then performs advanced processing to evaluate and correlate events to continually monitor how devices, users, and applications are performing.

Correlation of data is key since it allows for troubleshooting issues and analyzing network performance across both the overlay and underlay portions of the SD-Access Fabric. Other solutions often lack this level of correlation and thus lose visibility into underlying traffic issues that may affect the performance of the overlay network. By providing correlated visibility into both underlay and overlay traffic patterns and usage via fabric-aware enhancements to Netflow, SD-Access ensures that network visibility is not compromised when a fabric deployment is used.
SD-Access Benefits

The transformational capabilities of SD-Access make it possible to enable some of the following use cases:

**Automated Deployments at Scale**

SD-Access leverages controller-based automation build out large enterprise networks without requiring the network operator to have an intricate understanding of the underlying network forwarding constructs. SD-Access provides a single set of networking constructs that cater to all connectivity scenarios.

Most importantly, SD-Access provides this flexible, automated connectivity across large enterprise domains in a resilient manner that minimizes instabilities and reduces risks of downtime. SD-Access is based on a distributed framework to support horizontal scalability and does not require re-architecting as the scale of the deployment grows – whether it be a deployment of 50 users or 200,000+ users.

SD-Access also works and scales seamlessly across a large number of sites with automated inter-site connectivity, and extends to environments outside of traditional wiring closets such as connected workspaces, Operational Technology (OT) environments, and manufacturing floors.

As a result, SD-Access enables Fast IT/Lean IT initiatives critical for business agility by easily accommodating any new connectivity requirements with a common, consistent, and fully automated network.
Some of the applications of this use case are listed below:

2. Education: access to teaching and learning resources across remote campuses.

Integrated Wired and Wireless Infrastructure

The wireless data plane is distributed (i.e. is not centralized at the wireless LAN controller) and shares the same transport and encapsulation as wired traffic. This enables the ability to leverage capabilities of wired infrastructure for wireless traffic. For example, Multicast or First Hop Security and Segmentation results in a better overall user experience over wireless.

SD-Access wireless provides:

- **Distributed data plane**: The wireless data plane is distributed at the edge switches for optimal performance and scalability. The fabric allows this optimized data plane forwarding without bringing the hassles usually associated with distributing traffic forwarding, including spanning VLANs, subnetting, etc.
• **Centralized wireless control plane**: The same innovative RF features that Cisco has today in CUWN deployments will be leveraged in SD-Access wireless as well. Wireless operations stay the same as with CUWN in terms of RRM, client onboarding, and client mobility. This allows simplified IT operations for the wireless as the single wireless control plane is maintained in the fabric as well with seamless roaming across the fabric.

• **Simplified guest and mobility tunneling**: an anchor WLC controller is not needed any more and the guest traffic can directly go to the DMZ without hopping through a foreign controller.

• **Policy simplification**: SD-Access breaks the dependencies between policy and network constructs (IP address and VLANs), simplifying the way we can define and implement policies for both wired and wireless clients.

• **Segmentation made easy**: Segmentation is carried end-to-end in the fabric and is hierarchical, based on Virtual Networks (VNIs) and Scalable Group Tags (SGTs). The same segmentation policy is applied to both wired and wireless users.

SD-Access wireless provides an IoT-ready infrastructure allowing the IoT devices to be segmented across the enterprise in their own segments without interfering with the corporate network.
Some of the applications of this use case are listed below:

2. Education: Improve learning experience in classrooms.
3. Retail: Enhanced guest experience over store WiFi.

**Provide secure access to Users and Devices**

SD-Access provides topology-agnostic, identity-based methods to define access control and network segmentation policies. This simplifies policy definition, updates, and compliance reporting (Refer to the diagram below).

The automation framework translates the high-level business intent into low-level configuration of devices in the network infrastructure to enable rapid, consistent, and validated roll-out of policies throughout the network.

---

**DIAGRAM Simple and Secure Access**

**IT Simplicity**
- No VLAN, ACLs or IP Address management required
- Single network fabric
- Define one consistent policy

**Security**
- Simplified Micro-Segmentation
- Policy enforcement
Some of the applications of this use case are:

1. Healthcare: Keep patient, devices, and data secure.
2. Education: Create a secure campus.

**Correlated Insights and Analytics**

Issue resolution today is reactive, slow, and inefficient. The reasons could be fragmented tools (each with limited visibility), network complexity, user mobility, or even lack of consistent policies.

SD-Access provides deep visibility into networks by collecting and correlating fine-grained telemetry from a rich variety of sources such as syslog, SNMP, NetFlow, AAA, DHCP, DNS, etc. This provides IT with rich actionable insights to optimize network infrastructure and support better business decisions.
Some of the applications of this use case are listed below:

2. Education: ensure network uptime and performance during classroom changes.
3. Manufacturing: get new business insights from plant floors to make better IT decisions.
SD-Access Fabric
Fabric Components

As we begin our examination of the SD-Access Fabric, we need to review the various components that make up fabric deployment, examine the capabilities that they provide, and outline how the various components interact with each other to provide the entire SD-Access solution.

The following diagram outlines the main components that are part of SD-Access fabric deployment, and indicate the various positions that they occupy within a SD-Access fabric system.
Fabric Components and Terminology

**Fabric Control Plane Node**: The Fabric Control Plane node serves as a central database, tracking all users and devices as they attach to the fabric network, and as they roam around. The fabric control plane allows network components (switches, routers, WLCs, etc) to query this database to determine the location of any user or device attached to the fabric, instead of using a flood and learn mechanism. In this way, the fabric control plane serves as a "single source of truth" about where every endpoint attached to the fabric is located at any point in time. In addition to tracking specific endpoints (/32 address for IPv4, /128 address for IPv6), the fabric control plane can also track larger summarized routers (IP/mask). This flexibility helps in summarization across fabric sites and improves overall scalability.

**Fabric Border Node**: Fabric Border Nodes connect the SD-Access fabric to traditional Layer 3 networks, or to different fabric sites. Fabric border nodes are responsible for the translation of context (user/device mapping and identity) from one fabric site to another fabric site, or to a traditional network. When the encapsulation is the same across different fabric sites, the translation of fabric context is generally 1:1 mapped. The Fabric Border is also the device where the fabric control planes of different fabric sites exchange reachability and policy information.

There are two notable fabric border functions: one for internal networks and one for external networks. Internal borders advertise a defined set of known subnets, such as those leading to a group of branch sites, or to a data center. External borders, on the other hand, advertise unknown destinations, typically to the Internet (similar to the function of a default route). In an SD-Access fabric, an arbitrary number of internal borders can exist. The total number of external borders supported per SD-Access fabric is smaller (2 or 4, depending on the border node types chosen).

**Fabric Edge Node**: Fabric Edge Nodes are responsible for connecting endpoints to the fabric, and encapsulating/decapsulating and forwarding traffic from these endpoints to and from the fabric. Fabric edge nodes operate at the perimeter of the fabric and are the first points for attachment of users and the implementation of policy. It is to be noted that the endpoints need not be directly attached to the fabric edge node (refer to Extended Nodes).
An important point to note about fabric edge nodes is how they handle the subnets used for endpoint attachment. All subnets hosted in a SD-Access fabric are, by default, provisioned across every edge node in that fabric. For example, if the subnet 10.10.10.0/24 is provisioned in a given fabric, this subnet will be defined across all of the edge nodes in that fabric, and hosts located in that subnet can be placed on any edge node within that fabric. This essentially "stretches" these subnets across all of the edge nodes in that fabric, thus simplifying the IP address assignment, allowing fewer but larger IP subnets to be deployed.

**Fabric Intermediate Node:** Fabric intermediate nodes are pure Layer 3 forwarders that connect the Fabric Edge and Fabric Border Nodes and provide the Layer 3 underlay for fabric overlay traffic.

**SD-Access Extended Node:** SD-Access Extended Node is used to attach downstream non-fabric Layer 2 network devices to the SD-Access fabric (thus, extending the fabric). The extended node is a device such as a small switch (Compact switch, industrial Ethernet switch, or building automation switch) which connects to the fabric edge node via Layer 2. Devices connected to the SD-Access extended node use the fabric edge node for communication to outside subnets.

**Fabric Wireless LAN Controller (WLC):** The Fabric WLC supports fabric-enabled APs attached to the fabric, handling not only the traditional tasks associated with a WLC but also handling interaction with the fabric control plane for wireless client registration and roaming. It should be noted that a fabric-enabled wireless deployment moves the data-plane termination (VXLAN) from a centralized location (with previous overlay CAPWAP deployments), to the AP/fabric edge node. This enables distributed forwarding and distributed policy application for wireless traffic, while retaining the benefits of centralized provisioning and administration.

**Fabric Access Point (AP):** Fabric APs are attached to fabric edge nodes and connect wireless clients into the fabric network. Fabric APs allow for distributed wireless forwarding in the SD-Access architecture by encapsulating wireless user traffic into the VXLAN-based overlay to their adjacent fabric edge node where it is decapsulated, any necessary policies are applied, and then re-encapsulated to its ultimate destination within the fabric.
**Endpoint:** The devices that connect to the Fabric Edge Node are called Endpoints (EPs). EPs may be wired clients that directly connect to the fabric edge node, wireless clients attached to a fabric AP, or connect through a Layer 2 network via an SD-Access extended node.

**DNA Center:** DNA Center is the command and control system for the SD-Access solution, and houses the automated workflows required to deploy and manage SD-Access fabrics. DNA Center provides capabilities for both automation and assurance in a fabric deployment (described in more detail in the following chapters). DNA Center serves both brownfield and greenfield deployments.
Fabric Operation

Control Plane Operation

In SD-Access fabric, the Fabric Control Plane Node operates as the database tracking all endpoint connectivity to the fabric, and is responsible for the following functions:

- Registers all endpoints connected to the Edge nodes, and tracks their location in the fabric.
  - i.e. which edge node the endpoints are located behind.

- Responds to queries from network elements about the location of endpoints in the fabric.

- Ensures that when endpoints move from one location to another, traffic is re-directed to the current location.

Refer to the following diagram showing the control plane operation.
1. Endpoint 1 on Edge 1 will be registered to the Fabric Control Plane node. The registration includes endpoint 1's IP address, MAC address, and location [which is fabric switch Edge 1].

2. Endpoint 2 on Edge 2 will also be registered to the Fabric Control Plane node. The registration includes endpoint 2's IP address, MAC address, and location [which is fabric switch Edge 2].

3. When endpoint 1 wants to communicate to endpoint 2, Edge 1 will query the Fabric Control Plane node for the location of endpoint 2.

4. Upon getting the reply (endpoint 2 location is behind Edge 2) it will encapsulate the traffic from endpoint 1 using VXLAN, and send it to endpoint 2 (via Edge 2).

5. Once this traffic arrives at Edge 2, it will be decapsulated and forwarded along to endpoint 2.

6. The reverse applies when endpoint 2 wants to communicate back to endpoint 1.

**Data Plane Forwarding**

VXLAN requires an underlying transport network (the underlay). Underlay data plane forwarding is required to provide communication between endpoints connected to the fabric. The following diagram illustrates data plane forwarding in a VXLAN-encapsulated network.
SD-Access fabric doesn't change the semantics of Layer 2 or Layer 3 forwarding and allows the fabric edge nodes to perform overlay routing or bridging functions. As such, the edge nodes offer a set of different gateway functions as outlined below:

- **Layer 2 Virtual Network Interface** (L2 VNI): In this mode, frames from an L2 VNI are bridged to another L2 interface. The bridging will be done within the context of a bridge domain. A common implementation of a L2 gateway would use a VLAN as the bridge domain and will make the L2 VNI a member port of the VLAN. The edge nodes will bridge traffic between the L2 VNI and the destination L2 port in the VLAN.

- **Layer 3 Virtual Network Interface** (L3 VNI): In this mode, frames from an L3 VNI are routed to another L3 interface. The routing will be done within the context of a routing instance. A common implementation of an L3 gateway would use a VRF as the routing instance and will make the L3 VNI a member port of the VRF. The edge nodes will route traffic between the L3 VNI and the destination L3 interface in the VRF.
In order to provide client mobility and "stretching" of subnets, SD-Access leverages **Distributed Anycast Default Gateway**. This provisions the Layer 3 interface (default gateway) onto every edge node in the fabric. For example, if the 10.10.10.0/24 subnet was defined in the fabric, and the default gateway defined for that subnet was 10.10.10.1, then this virtual IP address (with a corresponding virtual MAC address) would be programmed identically on every edge node.

This significantly simplifies the endpoint deployment and facilitates roaming within the fabric infrastructure, since the default gateway is identical on any and every fabric edge node. This also optimizes traffic forwarding, as traffic from an endpoint going to an off-subnet destination is always L3-forwarded at the first hop. It is never hairpinned to a remote location for L3 traffic forwarding, as some older (non-fabric) stretched subnet solutions require.

In addition, the underlay network can be used to deliver multi-destination traffic to endpoints connected to a common Layer 2 broadcast domain in the overlay network. This includes broadcast and multicast traffic in the fabric. Broadcast traffic in SD-Access fabric is mapped to an underlay multicast group and sent to all the edge nodes within that common broadcast domain. This is described in more detail in the following chapters.

**Wireless in SD-Access Fabric**

There are two primary options for integration of wireless with SD-Access:

- **SD-Access Wireless**: provides full integration of wireless into the Fabric.
- **Traditional Wireless or Over the Top (OTT)**: legacy wireless traffic is carried over the fabric.

In the next sections, we describe the technical implementation of these two modes.
**SD-Access Wireless**

In SD-Access fabric, wired and wireless are part of a single integrated infrastructure and behave the same way in terms of connectivity, mobility, and policy enforcement. This brings a unified experience for users independently of the access media.

In terms of control plane integration, the Fabric Wireless LAN Controller notifies the fabric control plane node of all wireless client joins, roams, and disconnects. In this way, the control plane node always has all the information about both the wired and wireless clients in the fabric, and always serves as the "single source of truth".

In terms of data plane integration, the fabric WLC instructs the fabric access points to form a VXLAN overlay tunnel to their adjacent fabric edge nodes. This AP VXLAN tunnel carries the segmentation and policy information to/from the edge node, allowing connectivity and functionality identical to that of a wired host.

When a wireless client joins the fabric via a fabric AP, the fabric WLC onboards the endpoint into the fabric, and informs the control plane node of its MAC address. The WLC then instructs the AP to form a VXLAN overlay tunnel to its adjacent edge node. Next, the wireless client will obtain an IP address for itself via DHCP. Once that completes, the edge node will register the IP address of the wireless client to the control plane node (to form a mapping between the client MAC and IP addresses), and traffic to/from the wireless endpoint can begin to flow.

The fabric WLC is physically located outside the fabric, external to a fabric border node. This can be in the same LAN underlay as SD-Access, but external to the fabric overlay. This is because the WLC may connect either directly to the border node, or be multiple IP hops away (e.g. a local data center). The IP subnet prefix of the WLC must then be advertised into the underlay routing domain, for AP onboarding and management (via traditional CAPWAP control plane).

The fabric APs are connected directly to the fabric edge nodes in the fabric overlay. Alternatively, the APs may be connected to SD-Access Extended Nodes. The APs leverage the stretched subnet capability and anycast gateway functionality on the fabric
edge nodes. This allows all the fabric APs throughout the campus to be on the same subnet.

NOTE: The fabric WLC must be on a network that provides 20ms or less AP-to-WLC latency, since fabric APs operate in local mode.

Once fabric capability has been enabled on the WLC, the AP join process works as follows:

- The AP initializes and joins the WLC via CAPWAP – the same way it does today.
  - All management and control traffic such as AP image management, licensing, Radio Resource Management (RRM), client authentication, and other functions, leverage this CAPWAP connection.

- After the AP joins the WLC, the WLC checks whether the AP is capable of supporting fabric.
  - If it does, fabric capability is automatically enabled on the AP.
• Once the appropriate signalling is complete, the AP forms a VXLAN tunnel with the fabric edge node.

Fabric capability is enabled on a per-WLAN basis. The client subnet and L3 gateway are located on the fabric edge nodes in the overlay (in contrast with the current CUWN model, where they exist on the WLC).

When a client joins a fabric-enabled wireless network, the process works as follows:

• The client authenticates with the WLC on an SSID enabled for fabric.
• The WLC notifies the AP to use VXLAN encapsulation to the fabric edge node and to populate the appropriate VN/SGT for that client in the VXLAN packet.
• The WLC registers the client MAC address in the fabric control plane node database.
• Once the client receives an IP address, the existing CP entry is updated by the fabric edge node – and the MAC and IP address are mapped.
• The client is now free to start communications in the network.

**Guest Access in SD-Access Wireless**

Guest Access can be enabled in SD-Access Wireless in one of the two ways:

• WLC with separate VN for Guest
• Dedicated WLC as Guest Anchor

**Separate VN for Guest**

In this mode, the guest network is just another Virtual Network in SD-Access fabric. This leverages end-to-end fabric segmentation by using a separate VNI and SGTs for guest. This separates the guest data plane from the other enterprise traffic.

There are two ways to enable this model:

1. Use the same control plane and border as enterprise traffic
2. Use a separate control plane and border which is dedicated to the guest traffic
In this option, the Guest Network is just another Virtual Network in SD-Access fabric. This approach leverages end-to-end fabric segmentation using a VNI (and SGTs for different guest roles, if needed) to separate the guest data plane from the other enterprise traffic. The guest VN is extended from the border to the firewall via VRF-Lite in the DMZ.

In this option, separation is achieved at all levels for guests, thus isolating them from the enterprise users. Guest users will be registered in the dedicated Guest Fabric Control Plane. The fabric edge node queries the separate guest control plane node and forwards the traffic to the guest border encapsulated in VXLAN.
The existing WLC Guest Anchor solution continues to work as it does today. This mode can be used as a migration step when guest anchor controllers already exist in the DMZ. In this case, the mobility tunnel is formed between the foreign WLC and the guest anchor controller and the guest SSID is anchored at the anchor controller. All guests are tunnelled to the guest anchor by the foreign controller.

**Traditional Wireless or Over-The-Top (OTT)**

For backward compatibility, the current Cisco Unified Wireless Network (CUWN) or other traditional centralized wireless architectures are fully supported with SD-Access. In this solution, the wireless infrastructure rides on top of the SD-Access fabric architecture, but the wireless infrastructure is not aware of or integrated with the SD-Access wired network (hence the term "Over the Top") from a control plane, data plane, or policy plane perspective. This deployment method provides a graceful migration step toward fully-integrated SD-Access wireless.

The WLC connects to the SD-Access network either directly to (or multiple hops away from) the border.
**OTT-Flex Wireless Deployment**

In Flex Wireless Deployments, the wireless control/management plane is centralized at the WLC but the data plane is locally switched at the AP. SSIDs may either be locally-switched or tunnelled to the WLC. APs connect directly to the fabric edge node and trunk the wireless VLANs to the fabric edge node for the locally switched SSIDs. APs convert the packet format from 802.11 wireless to 802.3 Ethernet and forward the packets to the fabric edge node.

As a result, locally-switched wireless clients will be registered to the fabric control plane as normal fabric endpoints, and traffic forwarding for those clients will work exactly like other wired clients in the fabric network.

DNA Center provides the option to automate flex deployments in SD-Access using either the DNA Center UI or APIs.
Extended Node in SD-Access Fabric

Extended Nodes are small switches that run in pure Layer 2 mode, and do not natively support fabric technology. These Layer 2 switches will connect to a fabric edge node via traditional Layer 2 methods. The VLANs / IP subnets configured on the extended node switches will obtain similar policy segmentation and automation benefits that the fabric natively provides.

The fabric extends the appropriate subnets of the fabric to SD-Access extended nodes using 802.1q Layer 2 trunking. This allows the extended node to perform normal local switching. When traffic leaves the extended node, to the connected fabric edge node, the traffic benefits from the centralized policy and scalability of the fabric.
Fabric Considerations

There are various network underlay considerations to be aware when implementing SD-Access, that may impact the operation of the fabric overlay. The most important of these are summarized below.

**Maximum Transmission Unit (MTU)**

It is recommended to avoid fragmentation and reassembly of traffic between network devices. It is therefore required to increase the Maximum Transmission Unit (MTU) in the underlay network by at least 50 bytes, in order to accommodate the VXLAN header (or 54 bytes if an 802.1q header is also required), on all network devices connecting to the fabric underlay.

Jumbo frame support in the underlay network is strongly recommended if the overlay uses frame sizes larger than 1500 bytes. The recommended global or per-interface MTU setting for an SD-Access fabric deployment is 9100 bytes.

**Underlay Interface Addressing**

The recommended network interface and address design is Layer 3 routed point-to-point interfaces which can be addressed with a /30 or /31 subnet mask.

**Underlay Routing Protocol**

DNA Center LAN Automation will deploy a standards-based IGP routing protocol (IS-IS) to automatically to bring up the underlay.
Similarly, for manual underlay configurations, it is recommended to deploy the IS-IS routing protocol. Other routing protocols (e.g. OSPF) are also supported but may require additional configurations.

**IS-IS Deployment**

As mentioned, DNA Center will deploy IS-IS as the best practice underlay routing protocol. This link state routing protocol is gaining popularity for large-scale fabric environments, although has primarily been deployed in Service Provider (SP) environments.

IS-IS uses Connection Less Network Protocol (CLNP) for communication between peers and doesn’t depend on IP for this purpose. With IS-IS, there is no SPF calculation on link change. SPF calculation only occurs when there is a topology change, which helps with faster convergence and stability in the underlay. No significant tuning is required for IS-IS to achieve an efficient, fast-converging underlay network.

**OSPF Deployment**

If a manual (self-deployed) network underlay model is chosen, OSPF (Open Shortest Path First) would be a common choice in many enterprise deployments. Like IS-IS, OSPF is a link-state routing protocol. The OSPF default interface type used for Ethernet interfaces is “Broadcast,” which inherently results in a Designated Router (DR) and/or Backup Designated Router (BDR) election, thus reducing routing update traffic.

This is unnecessary in a point-to-point network. In a point-to-point network, the “Broadcast” interface type of OSPF adds a DR/BDR election process and an additional Type 2 Link State Advertisement (LSA). This results in unnecessary additional overhead, which can be avoided by changing the interface type to “point-to-point”.
Fabric Deployment Models

Multiple deployment options exist for SD-Access fabric. In this chapter, we will explore several of the options available.

- **Fabric Site**: a single fabric contained within a single site.
- **Fabric Multi-Site**: a common fabric across multiple sites.

**Fabric Site**

A fabric"site" is a portion of the fabric which has its own set of Control Plane Nodes, Border Nodes, and Edge Nodes.

Key characteristics of a single fabric site are:

- A given IP subnet is part of a single fabric site.
- L2 Extension is only within a fabric.
- L2 / L3 mobility is only within a fabric.
- No context translation is necessary within a fabric.

A fabric site is, in principle, autonomous from other fabric sites from the connectivity perspective.

The diagram below depicts a fabric site.
Many SD-Access deployments will be satisfied within the scale associated with a single-site fabric. However, some fabric deployments may need to scale to larger – or to smaller – sizes.

A given fabric site can have different scale characteristics:

- Large-scale fabric site: multiple horizontally-scaled devices, per fabric site.
- Fabric site in-a-box: all fabric functions are on a single device (site).

**Large Scale Fabric Site**

A fabric site is limited by the scale that it can provide, especially from the perspective of how many endpoints can connect. The endpoint scale depends on the Fabric Control Plane type, as well as other factors, such as DNAC and the choice of Border platforms. For example, a CSR router acting as Control Plane Node can support 200,000 IPv4 endpoints. This is the maximum number of supported endpoints per site.
A large-scale fabric site extends a single fabric site, so a larger number of endpoints can be supported. This is achieved by distributing the subnets across a group of control plane and border nodes at the site. By doing this, we can achieve very large scale networks. The following diagram depicts a large scale fabric site.

**Diagram**  
*Large-Scale Fabric Site*

**Wireless in a Large-Scale Fabric Site**

In a large-scale site design, the fabric is horizontally scaled to distribute multiple IP pools to multiple control plane and border node pairs (as shown above). The WLC is also enhanced to support this horizontal scale design, and a single WLC is allowed to communicate with multiple control plane nodes responsible for different IP pools in a fabric. To achieve fabric wireless scale, multiple WLCs can be added in the same fabric site and configured in the same mobility group to enable seamless roaming.
**Fabric Site In-a-Box**

A fabric site in-a-box allows the border node, edge node and control plane node functions to operate on the same fabric device. Thus, a small site can gain the advantage of fabric benefits, while still maintaining local resiliency and failover mechanisms. The following diagram depicts a fabric site in-a-box.

**Fabric Multi-Site**

An SD-Access fabric may be composed of multiple sites. Each site may require different aspects of scale, resiliency, and survivability. The overall aggregation of sites (i.e. the fabric) must also be able to accommodate a very large number of endpoints, scale horizontally by aggregating sites, and having the local state be contained within each site.

Multiple fabric sites corresponding to a single fabric will be interconnected by a Transit Network area. The Transit Network area may be defined as a portion of the fabric that has its own control plane nodes and border nodes but does not have edge nodes. Furthermore, the Transit Network area shares at least one border node from each fabric site that it interconnects. The following diagram depicts a multi-site fabric.
Role of the Transit Network area

In general terms, a Transit Network area exists to connect to the external world. There are several approaches to external connectivity, such as:

- Traditional IP network
- Traditional Wide Area Network (WAN)
- Software-Defined WAN (SD-WAN)
- SD-Access (native)

In the fabric multi-site model, all external connectivity (including Internet access) is modeled as a Transit Network. This creates a general construct that allows connectivity to any other sites and/or services.

The traffic across fabric sites, and to any other type of site, uses the control plane and data plane of the transit network to provide connectivity between these networks. A local border node is the handoff point from the fabric site, and the traffic is delivered across the transit network to other sites. The transit network may use additional
features. For example, if the transit network is a WAN, then features like performance routing may also be used.

To provide end-to-end policy and segmentation, the transit network should be capable of carrying the endpoint context information (VRF, SGT) across this network. Otherwise, a re-classification of the traffic will be needed at the destination site Border.

Fabric Control Plane state distribution

The local control plane in a fabric site will only hold state relevant to endpoints that are connected to edge nodes within the local fabric site. The local endpoints will be registered to the local control plane by the local edge devices, as with a single fabric site. Any endpoint that isn’t explicitly registered with the local control plane will be assumed to be reachable via the border nodes connected to the transit area.

At no point should the local control plane for a fabric site hold state for endpoints attached in other fabric sites (i.e. the border nodes do not register information from the transit area.) This allows the local control plane to be independent of other fabric sites, thus enhancing the overall scalability of the solution.

The control plane in the transit area will hold summary state for all fabric sites that it interconnects. This information will be registered to the Transit Area Control Plane by the border nodes from the different fabric sites. The border nodes register EID (Endpoint IDs) information from their local fabric site into the Transit Network Control Plane for summary EIDs only, further improving overall scalability.

NOTE: It is important to note that endpoint roaming is only within a local fabric site, and not across sites.

How to create a Multi-Site fabric?

Normally, when there are many small branches, the biggest challenge is how to manage these sites. Creating a separate fabric domain for each site is a cumbersome task. The creation of multi-site fabric is a three-step process:
1. Create Transit network(s)
Transit network creation depends on type of transit network.
   1. SD-Access transit networks are created by enabling Fabric Control Plane Node(s) for the transit network.
   2. SD-WAN transit networks are created using an SD-WAN protocol.
   3. IP transit networks are created using any traditional routing protocol (e.g. BGP).

2. Create Fabric site(s)
Creation of a fabric site involves the following steps (as described above):
   1. Add control plane node(s) for this site.
   2. Add border node(s) to this site.
   3. Add edge nodes to this site.

3. Connect local Fabric Site(s) to the Transit network(s):
Fabric site(s) are connected using local border node(s).

Wireless in Fabric Multi-Site
Fabric wireless is an integral part of the fabric multi-site design. Each local fabric site has its own dedicated WLC and is responsible for managing the wireless infrastructure at that local site. Since there is no Layer 2 mobility across sites in a multi-site design, the WLCs that are dedicated to each site are not configured in a mobility group. Hence, seamless roaming is not supported across sites.

IOT Deployment Models
As described earlier, SD-Access supports specific Layer 2 connected switches, known as SD-Access Extended Nodes, with indirectly connected endpoints.

Multiple SD-Access extended nodes may be directly or indirectly connected to a Fabric Edge node. These switches may be connected in one of the following ways:
- Connected over point-to-point links to an edge node.
- Connected over an STP or REP ring to an edge node.

The STP or REP ring-based deployment is important for IoT deployments where various types of sensors connect to the ports on the extended node. The Extended Node does all of the endpoint onboarding connected to its ports, but policy is only applied by the edge nodes. This means that the traffic between endpoints directly connected to the same extended node, or between extended nodes connected to a ring, do not enforce policy.

Thus, the support of fabric edge node allows the IoT devices to utilize the fabric benefits including Layer 2 extension and segmentation.
External Connectivity

Obviously, the SD-Access fabric will need to connect to external locations. Many external connection options exist, depending on the specific environment. Some common examples include:

- other campuses
- branch offices (over a WAN)
- data centers
- cloud networks.

For each of these external connection options, we will describe solutions for extending SD-Access policy elements (VNs and SGTs) to remote sites. The first aspect is VN, which is translated into a standard VRF format. The second aspect is the SGT, which may be transported natively, or re-classified at the remote site.

Let's begin with discussing WAN integration. There are four main WAN hand-off options:

1. SD-Access (LISP/VXLAN)
2. SD-WAN
3. MPLS-VPN
4. VRF-Lite over DMVPN

As described earlier, three architecture aspects need consideration:

- Control plane (routing/signaling protocols)
- Data plane (encapsulation)
- Policy plane (endpoint context).
SD-Access LISP/VXLAN Transport

In an SD-Access multi-site deployment model, the same control, data, and management plane is used, and the concept is nothing more than extending SD-Access over the WAN (or Metro Ethernet, which typically supports close geographical proximity of locations).

As described earlier, SD-Access multi-site can natively extend both the VN and SGT policy encoding within the same VXLAN encapsulation and LISP control plane, over any transport network (WAN or Metro) that supports IP routing. In this design model, the SD-Access border node can serve both border and WAN edge functions.

**NOTE:** SD-WAN transport is the long-term preferred design model for WAN environments, including for extending SD-Access domains. The SD-Access multi-site solution offers network designers with additional options for extending SD-Access domains to one or more close geographical locations, particularly for Metro Ethernet environments.
**SD-WAN Transport**

In an SD-WAN deployment model, VRF-Lite is used to extend the VN from the SD-Access Border node to the SD-WAN edge router.

SD-WAN encapsulation may not be able to transport the SGT ID. To overcome this, the remote SD-Access Border node can leverage the SGT re-classification method (an SGT can be defined for an incoming packet on either an interface/sub-interface or subnet), or leverage SXP to provision the SGT tags between SD-Access domains (but requires additional configurations and scale considerations).
**MPLS VPN Transport**

<table>
<thead>
<tr>
<th>DIAGRAM</th>
<th>MPLS VPN Transport Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Plane</td>
<td>SGT in VXLAN</td>
</tr>
<tr>
<td>Data Plane</td>
<td>VXLAN</td>
</tr>
<tr>
<td>Control-Plane</td>
<td>LISP</td>
</tr>
</tbody>
</table>

In the MPLS-VPN deployment model, VRF-Lite is used to extend the VN from the SD-Access border node (CE in an MPLS-VPN model) to the MPLS PE node.

MPLS encapsulation is unable to natively transport the SGT tag. To overcome this, the remote SD-Access border node can leverage the SGT re-classification method (an SGT can be defined for an incoming packet on either an interface/sub-interface or subnet), or leverage SXP to provision the SGT tags between SD-Access domains (but requires additional configurations and scale considerations).
VRF-Lite over DMVPN Transport

In the Dynamic Multipoint VPN (DMVPN) deployment model, VRF-Lite is used to extend the VN from the SD-Access border node to the DMVPN edge router.

DMVPN mGRE encapsulation is capable of carrying the SGT tag natively over the WAN. This offers a much simpler solution as there is no need to leverage SGT re-classification or SXP.

Data Center Connectivity

For data center interconnection, this book focuses on Application Centric Infrastructure (ACI) interoperability.

Cisco ACI is the data center architecture with centralized automation and policy-driven application profiles. Cisco ACI uses Endpoint Groups (EPGs) as the main policy
construct for defining policy within the ACI fabric. EPGs identify application workloads in the ACI fabric.

Cisco offers the ability to federate endpoint identifiers (SGT and EPG) beginning in Cisco ISE 2.1. Cisco ISE will share user selected SGTs to ACI, as well as read EPGs from ACI. The sharing of the SGT takes the form of writing SGT names into ACI fabric as EPG names at a specific ACI construct where they build policies for external connectivity (referred to Layer 3 Out).

ACI can then provide all of its policy services to relationships between the SD-Access SGTs and the ACI EPGs. Similar to what is described above, ISE reads EPGs and shares them to pxGrid ecosystem partners, which includes the DNA Center managing the SD-Access fabric. This allows SD-Access to build and enforce both user/device and application policies in the SD-Access fabric.

**Diagram**

Policy Group Identity Federation

NOTE: Some consideration in the ACI fabric is necessary since ACI supports multiple tenants (each tenant can have multiple VRFs). The recommended way to connect SD-Access to the ACI fabric is to have a shared services VRF applied across all of the
tenants, to provide a common Layer 3 external connectivity for them. ISE then writes all the SGTs into this shared VRF and the SGTs can be applied to all tenant policies.

**Diagram: Shared VRF between SD-Access and ACI**

An additional benefit of the SD-Access and ACI integration is that we can share IP/SGTs derived from ACI with other IT security partners (via the pxGrid ecosystem). This allows a normalized identification for users/devices and applications to be represented in telemetry, and used by partner systems such as Cisco Stealthwatch, and/or to be used in a security policy for functions such as the Cisco Web Security Appliance (WSA) and Firepower Next Generation Firewall.
Shared Services (DHCP, DNS, IPAM etc.)

In all network deployments there is a common set of resources needed by every endpoint. Here are the common examples:

- Identity services (e.g. AAA/RADIUS)
- Domain Name Services (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- IP Address Management (IPAM)
- Monitoring tools (e.g. SNMP)
- Data collectors (e.g. Netflow, syslog)
- Other infrastructure elements

These shared services will generally reside outside of the SD-Access fabric. These common resources are often called Shared Services. In the majority of cases, shared
services reside in the global routing table (GRT) of the existing network (and are not in a separate VRF).

NOTE: As previously described, SD-Access fabric clients operate in overlay virtual networks. Thus, if the shared services are part of the global routing space, some method of inter-VRF routing is required.

One option for inter-VRF routing is to leverage a "fusion" router. A fusion router is simply an external router, which performs basic inter-VRF leaking (import/export of VRF routes) to fuse the VRFs together. Refer to the diagram below.

Some fusion router design considerations apply, depending on whether the shared services are in GRT or VRF.

NOTE: Multi-Protocol BGP is the routing protocol of choice for this route exchange since it provides an inherent way of preventing routing loops (using AS_PATH attribute). Other routing protocols can be used, but require complex distribute-lists and prefix-lists to prevent loops.

Shared Services in the GRT:

- The fabric border node forms an eBGP routing adjacency with the fusion router, using the global routing table.
• On the border node, the same routing adjacency is formed in each VRF context (BGP address-family).
• On the fusion router, routes between the SD-Access VNs are then fused with the GRT of the external network.

Shared Services in separate VRF:
• A separate routing adjacency is formed between each BGP address family, between the border node and fusion router.

There are four main challenges using the fusion router method to achieve inter-VN communication:
• Route duplication – routes leaked from one VRF to another are programmed in the hardware tables, resulting in more TCAM utilization.
• Multiple touchpoints – manual configuration must be done at multiple points (wherever the route-leaking is implemented).
• Loss of SGT context – SGT group tags are not maintained across VRFs and must be re-classified once the traffic enters the other VRF.
• Traffic Hairpinning – traffic needs to be routed to the fusion router, and then back to the fabric border node.

SD-Access Extranet

SD-Access Extranet provides a flexible, and scalable method for achieving inter-VN communications and is explained below.

The advantages directly contrast the fusion router method above:
• Avoids route duplication – inter-VN lookup is done in the fabric control plane (software) that avoids duplicating hardware route entries.
• Single touchpoint – DNA-Center will automate the inter-VN lookup policy, making it a single point of management.
• Maintains SGT context – SGTs are maintained, since the inter-VN lookup is done on the control plane node (software).
• No hairpinning – inter-VN forwarding occurs at the fabric edge (same intra-VN) so traffic does not need to hairpin at the border node.

Another advantage is that, depending on the requirements, a separate VN can be made for each of the common resources that are needed (i.e. for Shared Services VN, Internet VN, and Data Center VN, etc.).

An important concept in SD-Access Extranet is the separation of provider VNs and subscriber VNs. A provider VN includes the commonly shared services reside (that are needed by other VNs). A subscriber VN is where clients (that need services) reside.

To understand how provider and subscriber VNs are used, consider the scenario below:

VRF RED is a Provider VN and VRFs BLUE and GREEN are subscriber VNs.
1. Host C1 connects to S1 on VRF BLUE.
2. Host C2 connects to S3 on VRF GREEN.
3. The DHCP Server is an endpoint that connects to S2 in VRF RED.
4. The Control Plane node registers the endpoint entries in its database.
5. The inter-VN policy dictates:
   - VRFs BLUE and GREEN should access resources in VRF RED
   - VRFs BLUE and GREEN cannot access each other’s resources.

6. Client C1 now wants to access DHCP server.
7. S1 receives the packet and sends a query to the control plane node.
   - It checks its database for DHCP in VRF BLUE but does not find an entry.
   - It refers to the extranet policy, which instructs it to check entries in VRF RED.
The Control Plane node does find the entry for the DHCP Server in VRF RED.

The Control Plane node then instructs S1 to encapsulate the packet in VRF RED and forward to S2.

- The result is cached by S1, for any future traffic destined for DHCP Server.

A similar sequence occurs for the client C2 in VRF GREEN to access resources in VRF RED.
Fabric Packet Walks

Now that we have reviewed the various SD-Access fabric components, and examined their operation and interactions, let's examine fabric packet forwarding and packet flows.

In this chapter the following packet walks are discussed:

- **ARP operation** (within SD-Access)
- **Unicast Wired-to-Wireless** (within SD-Access)
- **Wireless mobility** (within SD-Access)
- **Unicast to External** (between SD-Access and external networks)
- **Fabric Multicast** (in the overlay)
- **Native Multicast** (in the underlay)
- **Broadcast support** (within SD-Access)

We will examine why each packet walk is relevant in the context of the SD-Access fabric, and any notable aspects of that packet walk to overall fabric operation and use.

**ARP operation in SD-Access**

The SD-Access fabric provides many optimizations to improve unicast traffic flow, and to reduce the unnecessary flooding of data. One of the first optimizations is ARP suppression. While traditional ARP flooding is workable with the smaller-scale subnets deployed in a traditional enterprise network, this process would be very wasteful of bandwidth in an SD-Access deployment.

In SD-Access, subnets are populated on all fabric edge nodes by default, and endpoints in those subnets could reside anywhere in the fabric (or even roam between edge
nodes. ARP operation in SD-Access has been designed to improve the efficiency of this process in a fabric deployment.

In this scenario, a wired client (C1) has connected to a switchport of the edge node (S1). It has already obtained an IP address from DHCP. The client wants to communicate to another client (C2) connected in the same subnet, on a different edge node (S2). Refer to the following diagram.

1. Before it can start, client C1 sends out an ARP request to discover the MAC address corresponding with the IP address of client C2.

2. Edge node S1 processes this ARP request
   - S1 floods it out to the local ports in the same VLAN as the client that sent the ARP request.
   - S1 also sends a query to the control plane node to check whether it has the MAC address corresponding to the IP address of C2.
The control plane has the entry for C2’s MAC address, as well as the IP address, and returns the MAC address information to S1.

- S1 then queries the control plane node about where that MAC address is located.
- The control plane returns the remote switch’s IP Address where C2 is located currently (S2).
- S1 caches this information in its local cache (to suppress subsequent queries for this client).
- S1 then replaces the broadcast address in the ARP request, with the MAC address of client C2.

3 S1 encapsulates the directed ARP request in unicast VXLAN (making the broadcast packet a directed unicast) with a destination of S2.

- S1 applies the specific policy context (VN, SGT) and transmits the VXLAN frame to S2.

4 S2 decapsulates the VXLAN header from the incoming packet and knows that the packet is destined for C2 (which is local)

- S2 then forwards the ARP request to C2.
- Client C2 looks at the incoming ARP packet then responds with its MAC address in an ARP reply packet.
- S2 accepts the incoming ARP reply packet, encapsulates in VXLAN towards S1, and forwards it to S1.
- S1 decapsulates the VXLAN header and forwards the ARP reply packet to C1 (completing the ARP discovery process).

In this way, the SD-Access architecture optimizes ARP discovery and avoids unnecessary ARP broadcast flooding in the fabric.
Unicast Wired-to-Wireless

As described earlier, wired and wireless endpoints reside in the same common SD-Access fabric. It is important to understand how traffic flow between these endpoints works, within an SD-Access deployment.

In this scenario, a wired client (C1), is connected to a switchport of fabric Edge node S1. Another wireless client (C2), in a different subnet, is connected to an Access Point (AP) that is connected to fabric edge node S2. The MAC and IP address of both clients are already registered with the fabric control plane node. Refer to the following diagram.

1. When C1 wants to communicate with C2, it will send an IP packet with the default gateway IP address as the destination in the packet.
2. S1 processes this packet and queries the fabric control plane to resolve the location of client C2.
The control plane checks in its host database and returns the IP address of S2.
- S1 then caches this information (to suppress subsequent queries for this client).
- S1 applies the specific policy context (VN, SGT) and transmits the VXLAN frame to S2.

S2 receives the packet and decapsulates the VXLAN header.
- S2 examines the underlying packet that C1 sent to C2, to locate C2 (which is connected the AP).
- S2 re-encapsulates the packet in VXLAN, with the policy context (VN, SGT) and forwards it to the AP.

The AP decapsulates the VXLAN header, and converts the packet to 802.11 format.
- The AP then forwards the packet (via RF) to the wireless client.

NOTE: If C2 were a wired client, then S2 will decapsulate the VXLAN header and simply forward the original packet out of the port where C2 is connected (i.e. wired-to-wired unicast).

**Wireless Mobility**

Wireless mobility is handled within the context of the SD-Access fabric itself, with wireless endpoint mobility handled between the WLC and the fabric control plane node. The following outlines how this mobility within the SD-Access fabric takes place.

In this scenario, consider two wireless clients (C1 and C2) are connected to different APs (AP1 and AP2 respectively) on the same fabric edge node S1. Assume that there are already communications occurring between the two clients.
**Intra-Switch Roaming**
Refer to the following diagram.

1. C2 roams from AP2 to AP1, on S1.
   - Since this is a roam within the same edge node, no additional signalling needs to occur in the fabric.

2. The MAC address table on S1 gets updated using the L2 frames sent by AP2.

**Inter-Switch Roaming**
Refer to the following diagram.

1. Now client C2 roams from AP2 on S2 to AP3 on S3.
   - The fabric APs and WLC process the client roam first.
2 The WLC notifies the fabric control plane node of the new location, on AP3.
   - The fabric control plane then updates its database with the new location, on S3.

3 The control plane updates the new edge node, the old edge node, and the border nodes with the new location of C2.

4 Communication continues between C1 and C2.

**Diagram: Wireless Mobility – Inter-Switch**

**Unicast to External Networks**

Naturally, there will always be traffic which needs to flow between the SD-Access fabric endpoints and endpoints located outside the fabric, in external networks. These traffic
flows will take place via the fabric border nodes. The following outlines how this forwarding takes place.

In this scenario, C1 is connected to S1. C1 wants to communicate with a host (C2) which is not in the SD-Access fabric (the host is external to the fabric), located either in a data center or on the Internet. Refer to the following diagram.
C1 sends the packet to S1, which is the default gateway for C1, destined to an external IP address C2.

2 S1 queries the control plane node for that the destination IP address.
   - The control plane replies in the negative (no match), since it cannot find a matching entry in its database.

3 S1 then encapsulates the original packet in VXLAN, with the policy context (VN, SGT), and forwards it to the external border.

4 The external border decapsulates the VXLAN header and does an IP lookup for the destination (using route-leaking or extranet)
   - If the destination route is in the global routing table, it forwards the packet to the next-hop router.
   - If the destination route is another VRF, it adds the appropriate VRF and forwards the packet to the next-hop router.

Fabric Multicast in the Overlay

Multicast traffic forwarding is used by many applications in enterprise networks today, to simultaneously distribute copies of data to multiple different network destinations. Within an SD-Access fabric deployment, multicast traffic flows can be handled in one of two ways (overlay or underlay), depending on whether the underlay network supports multicast replication, or not.

First examine when the underlay network does not support multicast replication.

In this case, the first SD-Access fabric node that receives the multicast traffic (also known as the head-end) must replicate multiple unicast copies of the original multicast traffic, to each of the remote fabric edge nodes where the multicast receivers located (i.e. the original multicast packet is encapsulated into a VXLAN unicast packet). This approach is known as head-end multicast replication.
NOTE: The same process applies for multicast sources connected to the SD-Access fabric, or from an external network.

In this scenario, consider client C1 connected to edge node S1. There is a multicast source (MS1) in the external network (outside of the border node). PIM Sparse-Mode operation is used, and the Fabric Rendezvous Point (RP) in this case is on the border node. In this example, there is no multicast configured in the underlay network. Refer to the following diagram.

**Diagram: Multicast Head-End Replication**

- Multicast Source
- External Network
- S1
- SDA Fabric
- C1
- IGMP Join
- Unicast VXLAN
- PIM Join
- IGMP Join
- Source Packet

---

SD-Access Fabric  88

---
1. S1 processes the IGMP Join from C1, for multicast group 225.1.1.1.
   - S1 sends a corresponding (*,G) PIM Join in the overlay (VXLAN encapsulated) towards the Fabric RP.

2. The Fabric RP creates a (*, 225.1.1.1) state in its Multicast FIB (MFIB), with an outgoing interface list entry of S1.

3. The multicast source MS1 starts transmitting data destined to 225.1.1.1, which is registered with the Fabric RP.
   - The Fabric RP creates a specific (MS1, 225.1.1.1) state in its MFIB, with S1 in the outgoing interface list.

4. The Fabric RP encapsulates the original multicast packet in VXLAN.
   - In this case, the destination IP address is S1 (unicast).
   - Traffic is then forwarded in the overlay directly to S1.

5. S1 receives and decapsulates the VXLAN packet, and forwards the original packet to C1 (based on the IGMP join in Step 1).
   - If there are 10 receivers for this traffic on S1, it is still a single stream replicated by the head-end (Border) node.
     - S1 performs local replication for all local receivers (e.g. 10, above) interested in this multicast group.

   - If there are multiple receivers connected to multiple remote edge nodes, the head-end node will make a separate (unicast) copy for every edge node that has local receivers (based on a PIM join, as in Step 1).
     - Each remote edge node performs local replication for its local receivers.

The head-end multicast replication approach provides an efficient multicast distribution model, for networks that do not support multicast in the underlay. The
main disadvantage is the potential workload of replication required of the head-end node.

**Native Multicast support in Underlay**

Another example is when the underlay network does support multicast replication.

This approach allows for greater efficiency in multicast traffic handling since the multicast traffic can be replicated “natively” by the underlay infrastructure to all of the fabric edge nodes (i.e. the original multicast packet is encapsulated into a VXLAN multicast packet). This significantly reduces the workload for the ingress (head-end) edge node and distributes the multicast replication load in the network.

Consider the same scenario as above. Client C1 is connected to edge node S1. There is a multicast source (MSI) in the external network (outside of the border node). PIM Sparse-Mode operation is used (also known as Any Source Multicast or ASM), and the Fabric Rendezvous Point (RP) in this case is on the border node. In this case, though, there is also multicast operating in the underlay.

Cisco SD-Access supports Source-Specific Multicast (SSM) only in the underlay. Refer to the following diagram.
1. S1 processes the IGMP Join from C1, for multicast group 225.1.1.1.

2. S1 sends two PIM Joins. S1 first sends an ASM join, in the overlay, to the Fabric RP for the group (225.1.1.1).
   - The RP creates an ASM group (225.1.1.1) in the overlay and maps to an SSM group (e.g. 232.1.1.1) in the underlay.
   - S1 then sends an SSM join, in the underlay, to join the mapped group (232.1.1.1).
- All remote edge nodes interested in 225.1.1.1 will join this underlay group (232.1.1.1).

3 The multicast source MS1 starts transmitting data destined to 225.1.1.1, which is registered with the fabric RP.

- The fabric RP creates a specific (MSI, 225.1.1.1) state, which is mapped to 232.1.1.1.

4 The fabric RP encapsulates the original multicast packet in VXLAN.

- In this case, the destination IP address is 232.1.1.1 (multicast).
- Traffic is then forwarded in the underlay to all nodes joined to this group.

5 SI receives and decapsulates the VXLAN packet, maps the outgoing interface list for 225.1.1.1, and forwards the original packet to C1 (based on the IGMP join in Step 1).

- SI performs local replication for all local receivers interested in this multicast group.
- If there are multiple receivers connected to multiple remote edge nodes, the head-end node replicates once to the underlay multicast group. This multicast packet is replicated natively, by the underlay and forwarded to all the fabric nodes.

The advantage in this mode is that the head-end node is not solely responsible for all the replications to fabric edge nodes, and instead relies on the native Multicast capabilities of the network underlay.

**Broadcast in SD-Access**

For some traffic and application types, it may be desirable to enable broadcast forwarding within the SD-Access fabric.
By default, this is disabled in the SD-Access architecture. If broadcast propagation is required, it must be specifically enabled on a per-subnet basis. An underlay multicast group is associated (on a per-subnet basis) within the VN, and all fabric nodes will join this multicast group.

NOTE: This function requires support for multicast in the underlay network.

Whenever a broadcast frame is received by a fabric edge node, it is then encapsulated in VXLAN and forwarded to all remote edge nodes, via the underlay multicast group. The remote edge nodes will then decapsulate the original broadcast frame, and forward it to all local switchports in the appropriate subnet.
DNA Center Overview

DNA Center is a centralized operations platform for end-to-end automation and assurance of enterprise LAN, WLAN, and WAN environments, as well as orchestration with external solutions and domains. It provides the network administrator to use a single dashboard to manage and automate the network.

DNA Center provides the IT operator with intuitive automation and assurance workflows that make it easy to design network settings and policies, and then provision and assurance the network and policies along with end-to-end visibility, proactive monitoring and insights to provide consistent and high-quality user experience.

Architecture Tenets

DNA Center has been designed to scale to the needs of the largest enterprise network deployments. It consists of both a network controller and a data analytics functional stack to provide the user with a unified platform for managing and automating their network. DNA Center has been built using a micro-services architecture that is scalable and allows for continuous delivery and deployment.

Some of the key highlights of DNA Center include:

- Horizontal scale by adding more DNA Center nodes to an existing cluster.
- High availability – for both hardware component and software packages.
• Backup and restore mechanism – to support disaster recovery scenarios.
• Role-based access control mechanism, for differentiated access to users based on roles and scope.
• Programmable interfaces to enable ISVs, ecosystem partners and developers to integrate with DNA Center.

DNA Center is cloud-tethered to enable the seamless upgrade of existing functions and additions of new packages and applications without having to manually download and install them.

**DNA Center Automation**

The primary goal of DNA Center Automation workflows is to transform the network admin’s business intent into device-specific network configurations. The DNA Controller consists, at a high level, of the Network Information Database, policy and automation engines, and the network programmer.
The controller has the ability to discover the network infrastructure and periodically scan the network to create a single source of truth that includes the network device details, software images running on the system, network settings, site definitions, device-to-site mapping information, and so on. This also includes the topology information that maps the network devices to the physical topology along with the detailed device-level data. All this information is stored in the Controller Network Information Database.

The policy engine provisions various policies across the enterprise network for Quality of Service / application experience and access control policies. The automation engine provides an abstraction layer for the entire enterprise network using the service and policy framework and leveraging device-specific data models etc. Finally, the network programmer service does the provisioning on the network device.

**DNA Center Assurance**

DNA Center uses advanced machine learning and analytics to provide end-to-end visibility by learning from the network infrastructure, clients connected to the network, and other contextual sources of information. DNA Center has an in-built data collector framework that is able to ingest data coming from a variety of sources.

All of the network infrastructure data is obtained via streaming telemetry mechanisms designed to optimize network load and reduce the delay in receiving data from the network layer. In addition to this, the data collectors are all built to gather data from various contextual systems such as Cisco ISE, ITSM and IPAM systems. The collectors are dynamically deployed on the basis of network device capability and can scale horizontally as needed.

All of this data is processed and correlated in real-time using time series analysis, complex event processing, and machine learning algorithms. The data is then stored within the DNA Center to provide meaningful assurance, troubleshooting, insights and trending information via the Assurance workflows.
SD-Access Policy
Policy and Services Overview

**Definition of Policy in the context of SD-Access**

In any discussion involving policy and services, the starting point is always the business drivers that create the requirement. In the past, the only business requirement of the enterprise network was to provide fast, highly available connectivity (also known as access). With trends in computing and networking over the past several years, both services and policies have evolved. Now the enterprise network policy must meet new requirements to support greater agility, flexibility and increased security.

In the following section, we will focus on a top-of-mind requirement, security, as an example of how SD-Access policy can address some of the current challenges in enterprise networks. It is important to note that a similar set of requirements and challenges exist for other network services and policies, such as Quality of Service (QoS), packet capture, traffic engineering, and so on, and SD-Access addresses those in a similar way.

**Business Drivers**

One of the normal business requirements that drives an SD-Access deployment is regulatory compliance for either industry reasons (PCI, HIPAA, etc.) or corporate compliance reasons (risk mitigation). Multiple requirements can exist within an organization. For example, a healthcare company that not only must be compliant to national regulations (HIPAA in the U.S.) but also PCI compliance requirements, while also wanting to mitigate risk to patient care by isolating their medical devices.

**Policy Scenarios**

Below is a set of sample requirements for a common healthcare network – these will be used as the framework for illustrating how SD-Access can solve the requirements while providing business agility, flexibility and lower operational expense.

As described above, the starting point is to evaluate the business drivers and requirements. For example:
• **Secure patient care**: Only allow approved medical users and medical devices access to the medical network.

• **Secure business-critical applications**: Identify all users endpoints as they access the enterprise network -and- only allow approved users and devices access to the general enterprise network.

• **Regulatory compliance requirements**: Only allow approved users or devices access to specific endpoints, servers and applications within the scope of PCI compliance.

• **Provide patient care**: Provide a guest network that is isolated from the enterprise and medical network.

Traditionally, the next step is to evaluate the network to understand where each of the primary resources noted above is located.

For example:

- Where are the medical devices located in the network?
- Where are the servers and applications within scope for PCI?
- Where are the medical users located in the network?

If the enterprise was fortunate, they would be able to associate all of the resources in question to a clear set of IP address subnets. This would allow them to build network objects which represent the association between a subnet and a human-readable name.

Here are some examples:

- 192.0.2.0/24 = MRI_devices
- 192.16.1.0/24 = Imaging_Servers
- 198.51.100.0/24 = PCI Applications
- 10.1.100.0/24 = Staff
- 10.1.200.0/24 = Guests
Policy Construction

The network architect would then need to build relationships between these network objects and a set of permissions (i.e. an access control policy, for all of the subnets in the environment). Typically, this is accomplished by using a security management system. Security management systems (for example a firewall or an ACL management system) provide a human-readable abstraction that maps the relationship between the IP prefixes and a "network object".

The network architect would then build access control rules between the network objects, for a specific protocol (IP, TCP, UDP, etc.) and port (http, https, etc.), and then a resulting permission (permit or deny) between the objects.

**DIAGRAM**  
Policy Construction Example

In order to guarantee policy enforcement, the network administrator needs to design the network in such a way as to direct the relevant traffic (for each subnet) to a corresponding policy enforcement point (e.g. distribution switch using ACLs, campus firewall, etc.). The management system would then use the network objects to program the IP addresses back into the policy enforcement point.

In most cases, all of the telemetry that results from an access control security policy is then represented as logs, flow data, hit counters, etc entirely as IP addresses. This
means that all information produced by the policy enforcement points is produced in ways that are only relevant to the network constructs, but not to policy constructs. Which also means that any security management or assurance products must again translate the network constructs back into policy constructs, across multiple enforcement points in the enterprise.

This becomes a very complicated exercise since it normally requires handling of multiple formats of telemetry and different aspects of data. This complicated correlation is needed to perform relatively simple tasks, such as, "IP address 1 (which is part of network object A) is currently communicating to IP address 2 (which is part of network object B), in this log, which means that there is a violation of security policy X" (as proven by having completed this sentence).

---

**The bottom line**

It is very complex to map the network object (VLAN/subnet) to a policy object, and retain relevance.

---

**Implementing Policy**

NOTE: There is an inherent assumption of what is described above: if you connect a device to the subnet, you inherit all the security access of the subnet.

Remember that the traditional purpose of the enterprise network is to provide fast and highly available access. This has several critical policy implications.

For example:

- There is no network challenge or validation to anyone connecting to different parts of the network, within the campus, data center or branches.
- If you could plug into the right port in the wall, then you could be classified by the security system as an MRI device.

Wireless changed this by introducing a device and identity challenge but did not change the traditional mapping of IP subnets to network objects for security permissions. Wireless also introduced user and device mobility, which became a
challenge to this tight coupling of network topology with security policy because a user and/or device could show up in any part of the network.

In addition, all of the work above needs to be repeated for the addition of IPv6 addresses to a network, along with some new challenges.

- There are more network scopes and aggregate subnets in IPv6, and each user and/or device may use multiple IPv6 addresses.
- IPv6 addresses are often felt to be harder to read and recall than IPv4, due to the length and inclusion of hexadecimal (alphanumerics).
- Depending on the security management tool, this may require creating separate IPv6 network objects and/or upgrading the software.

When the policies are created and applied, they are often locked into the management tool where they were created. While software-defined networking has led to the creation of networks and applications via automation, this automation has not easily extended into security policy. In many cases, the automation is either incomplete (workload only, not for users/devices in the branch, etc), or it is vendor-specific.

In most cases, the network objects and policy are not extended to multiple kinds of enforcement points (i.e. firewall and switches or routers). Different types of enforcement points are often managed by different management systems, and it takes manual effort to synchronize the policy between the systems. There are some third-party tools focused on multi-platform and multi-vendor management but they are limited to common constructs and require yet another level of operational complexity.

Furthermore, as we move up into the application layer of security technology and operations, there is relevance for the network security objects. For example, assume the network security policy has allowed a device to communicate to the Internet (generically). Unless the network security policy management console and the advanced malware management console manually share the relevance of the network object to the broader enterprise, the advanced malware console will not have any awareness of the business relevance of an endpoint in their generated alarms. Hence, if a device that has been deemed critical to the business is compromised by malware, and
the malware sensor detects the exfiltration, the malware operator will most likely not see a high-level alert about the event.

Another challenge when dealing with policy is that many Access Control Entries (ACEs) in ACLs on firewalls and/or switches and routers will remain unchanged (or not-optimized) and grow continually over time because the network administrators do not actually know what business drivers or requirements the rules are intended to enforce.

**Policy Considerations**

The primary challenge with the current approach is that we work from objects (IP addresses), to business-relevant objects (network objects), and then back to objects (IP addresses), with no way to carry business relevance.

For example:

- Policy-related telemetry lacks human-readable business relevance (logs and flow statistics only use IP addresses and not user context).
- It is difficult to derive actionable intelligence from what the network telemetry is telling you about the policy.
- Reliance on multi-platform or multi-vendor tools to correlate between the constructs.
- Time-consuming, complicated and error-prone processes can lead to gaps in implementation and/or enforcement.

Current enterprise technologies also lack scalable enforcement for lateral spread within a VLAN/Subnet. With recent security events, there is a renewed focus on being able to control traffic within, and between, groups within an enterprise. There have been numerous security incidents involving IoT devices and user devices, where the lack of controls within a VLAN/subnet has led to malware and ransomware infecting business-critical assets.
Due to this natural LAN behavior, new traffic steering mechanisms were introduced to direct devices within the same VLAN/subnet to an enforcement point (e.g. private VLANs, etc.). This also means that to control lateral spread within a subnet, you must create a new ACL policy per VLAN/subnet, even if large parts of these IP subnets are really the same network object.

Finally, with the introduction of mobility, network administrators can no longer assume any given static IP subnet/VLAN structure can be relied upon to accurately represent a given set of end users/devices for the purposes of policy. Nor can network administrators try to manually keep up with the rate of addition and change with mobile users/devices.

In the following section, the reader will learn how Software-Defined Access uniquely solves the challenges described above.
Policy Architecture

Policy Enforcement in SD-Access

As described earlier, the SD-Access fabric provides two key segmentation constructs – VNs for macro segmentation, and Groups for micro segmentation – to be combined together to meet the policy definition needs of the organization.

Policies in SD-Access are defined on the basis of logical groupings of users, devices, things or applications and as a relationship between two groups, and further defines the access control rules based on L3 and L4 classifiers. For example, it is possible to create a policy defining the "physical security cameras" group to be denied access to the "badge readers" group, or the "medical devices" group to have access only from the "doctors" group.

Both wired and wireless policies are centrally defined and managed in SD-Access using DNA Center. They are enforced at the fabric edge and border nodes, based on the user/device identity, in a topology-agnostic manner. The group classification for the endpoint is embedded into the fabric data plane and carried end-to-end with the SD-
Access fabric, so policy for the traffic can be enforced irrespective of its source location.

For stateful inspection, group-based policies can also be applied at SGT-aware firewalls or web-proxies.

**Endpoint Grouping at Access**

Cisco Identity Services Engine (ISE) helps establish the identity of endpoints connecting to the network through a variety of mechanisms, such as 802.1X, MAC addresses, profiling, Active Directory login, and captive portals.

Once the identity of the endpoint is established, Cisco ISE also defines the rules association of endpoint identity to the Group. Attributes from Active Directory groups can be used in defining the group classifications in ISE, for use in SD-Access. These groups are imported into DNA-Center so that policies can be viewed and administered from the DNA Center user interface.
DNA Center is also capable of gathering endpoint identity information from external NAC and AAA systems and using the externally derived identity to map the endpoints into groups.

For environments that are not enabled for identity-based access through any of the above mechanisms, DNA Center allows the network administrator to statically define associations between access ports and groups.

**Application Groups**

Policies can be defined and implemented for users or endpoints to applications in DNA Center by classifying the external applications into groups based on their IP address or subnets. This is especially relevant in data centers where the applications are grouped for security reasons into pre-defined subnets.

For data centers based on Cisco’s Application Centric Infrastructure (ACI), the endpoint groups from SD-Access can be imported by the APIC controller in ACI. Policies can then be defined based on the same group-policy model end-to-end from user access to the application. This results in highly scalable, automated, simplified policy implementation that caters to user or workload mobility.

Cisco’s Cloud Policy Platform enables workloads in public cloud environments such as AWS, as well as those in hybrid cloud environments, to be mapped into groups that can be imported into DNA Center. DNA Center can thereby define and implement access control policies between user/device endpoints and the applications in public/hybrid cloud using the same group-based policy constructs. These group policies can be instantiated at a policy enforcement point such as the fabric border or a compatible firewall.
Policy Benefits

Aside from lowering the complexity and overall costs of operating the network, SD-Access Automation and Assurance implements a policy-driven model for network operations that reduces the time required to introduce new services and improve overall network security. These benefits are further discussed below.

Decouple Policy from Infrastructure Design

Similar to the way SD-Access abstracts network connectivity through VXLAN overlays, SD-Access also abstracts the notion of policy and decouples it from the underlying network topology. This allows for network design changes without a need for the operator to manually define and update individual policy elements.

Since SD-Access leverages the fabric network infrastructure for policy enforcement, complex traffic engineering mechanisms to forward traffic to firewalls are no longer necessary, and thereby reduce IP-ACL sprawl in firewalls.

The decoupling of the policy from the network topology enables more efficient operations and enables the network to be more effectively used to enforce policies. This leads to a number of associated business benefits around quicker time to enable new business services, enabling seamless network mobility, and overall reduction of effort in the day-to-day network administration.

Simplified Policy Definition

Management of access control policies on the basis of logical, business relevant, and human-readable groups simplifies ongoing operations and reduces the security risk. It also reduces the time and effort required to demonstrate compliance and simplifies the audit process.
Policy Automation

The dynamic association of an endpoint to its group based on its identity reduces the operational overhead required to ensure that the endpoints are on the appropriate network segment. This also enhances overall enterprise security, especially in environments where users and devices are mobile.

The complexity and time needed with the older methods is linear to the number of devices in the enterprise network and execution tasks on each of those devices. In SD-Access, these activities are not only simpler, but also far faster to execute, and much easier to design, deploy, operate, and understand.

Policy-Based Enterprise Orchestration

The SD-Access policy model provides a platform in which customers can develop a vast number of applications, targeting use cases including segmentation, security, compliance, and responses to real-time security threats, as well as the ability to offer a variety of services within the fabric.

Through the use of APIs in DNA Center, abundant network telemetry sources, and intelligent machine learning, SD-Access can leverage the “closed-loop” model concept
(shown in the diagram above). This closed-loop model can be adopted with SD-Access and will support a multitude of use cases, each leveraging the SD-Access policy model as the method for deploying the “actionable” intent into the SD-Access fabric.
Policy in Action

Consider a Security Operations team's ability to leverage the SD-Access policy model to respond to varying levels of vulnerabilities, beyond user access. For example, assume a new vulnerability has been identified for a popular host OS, and a user of that host logs on to the network. Through a management agent, that host OS is identified as not yet having patched the vulnerability. Based on that criteria, the management agent can identify the vulnerability as a "threat" level, and through APIs into the SD-Access fabric apply a "threat" level policy.

For example, the policy could instantly deny that user access to any business-critical systems throughout the enterprise network, while still allowing them access to non-critical systems and external networks such as the Internet.

This example highlights the power of the policy model within SD-Access. Central control from DNA Center, abstracted in the policy model from network topology, is applied to each network element where policy enforcement actions are required. Attempting the same capabilities with today's network operations tools and methods is simply not possible without hugely time-consuming tasks by human network operators, and could take days.

SD-Access also offers the flexibility for third-party applications to create, instantiate, and push policy into the fabric through an open set of APIs in DNA Center. Customers could use these APIs in environments that are leveraging applications such as security information and event manager (SIEM) systems. While a SIEM system may not configure the network, integrating it with SD-Access fabric that can drive policy changes in the network can help the security operator accelerate response to events identified by the SIEM.

As high-risk events are detected within the SIEM, it could then call APIs to DNA Center requesting a creation or modification of an SD-Access policy to "quarantine" a specific set of users/ports to rapidly contain the threat or to instantiate an ERSPAN (traffic copy) session for further analysis.
The API calls to DNA Center have triggered the traffic copy policy, and API calls to ISE have quarantined the user.
SD-Access Automation
Automation and Orchestration in DNA Center

Automation and Orchestration, as defined in the Software-Defined Access overview section, bring the "Software-Defined" concept to the "Access" network, translating the user's "intent" into meaningful configuration and verification tasks.

Cisco SD-Access uses controller-based automation as the primary configuration and orchestration model, to design, deploy, verify, and optimize the wired, wireless and security network components. With DNA Center, IT teams can now operate at an abstracted level that is aligned with the business objectives and not worry about the implementation details. This results in simplifying operations for the IT teams by minimizing the chances of making a human error and more easily standardizing the overall network design.

Cisco DNA Center provides multiple forms and levels of automation and orchestration, for both non-fabric and fabric-based components. Below is a brief list of the key principles and concepts of Cisco DNA automation and orchestration:

**Agility**: Reduce the time required to design, deploy and/or optimize a network environment. DNAC makes agility real by:

- Centralizing design: Generating, organizing and managing a set of common and/or unique network designs for different operating environments, including specific requirements for global and local network device settings.
- Automating deployment: Rapidly deploying configurations to multiple devices, and providing verification of deployment
- Optimizing design: Ensuring consistency of network state and configurations at scale, to match the desired operator objectives.

**Reliability**: Consistent deployment of prescriptive "best practice" network configurations. DNAC brings reliability with:
• Configuration best-practices: Mature and tested designs and configurations ensure consistent predictable behavior.
• Profile or template-based configuration: Different designs and configurations organized into easy to manage sets of profiles or templates.

**Simplification**: Minimize the complexity of configuring and integrating multiple devices. DNAC introduces simplification by:

• Centralizing management: Providing a central location for all of the functions required to design, deploy and manage multiple network components and/or external services, that can serve as the single source of truth, in a single-pane-of-glass
• Reducing touchpoints: Reducing the traditional box-by-box configuration and management tasks, and providing a single, centralized interface for network operations.
• Programmable interfaces (APIs): Allowing operators to automate network operations in their own customized manner, while leveraging a centralized platform to maintain and drive the changes in network state.

**Abstraction**: DNA Center uses easy-to-understand concepts and constructs that abstract out the underlying feature and technology implementation specifics of the network infrastructure. DNA Center provides this through simple, technology agnostic workflows, supported by views of both physical and logical network topology.

**What is Automation and Orchestration in the context of Cisco SD-Access?**

Cisco Software Defined Access (SD-Access) applies the key concepts of automation and orchestration to an enterprise campus network. This includes several major technologies, such as wired access, wireless access, as well as services and policies for security and application optimization. Cisco SD-Access automation and orchestration can be divided into two main categories: network underlay (or non-fabric) and fabric overlay.

Below is a key set of workflows for **Network Underlay**: 
• **Global and site settings**: Hierarchical management of network configurations (e.g. servers, IPAM, etc) for different sites.

• **Device discovery (existing networks)**: Automated discovery and inventory of existing network devices.

• **LAN automation (new networks)**: Automated discovery, provisioning, and inventory of new network devices.

Below is a key set of workflows for **Fabric Overlay**:

• **Fabric sites**: An automated configuration of a set of fabric-enabled network devices, with a common fabric control-plane and data-plane.

• **Fabric device roles**: An automated configuration of network devices operating various fabric functions, including Control Plane, Border, Edge, WLC, AP or Extended Nodes.

• **Virtual networks**: An automated configuration of functions to enable virtual routing and forwarding segmentation in the fabric overlay.

• **Group-based policies**: An automated configuration of functions to classify and/or enforce group-based policies in the fabric overlay.

• **Host onboarding**: An automated configuration of functions to onboard clients, including static or dynamic VN, IP pool and Scalable Group assignment, SSID, L2, etc.

• **Multicast services**: An automated configuration of functions to enable IP multicast distribution in the fabric overlay.

• **Pre-verification**: A tool to verify capability and support of network devices, prior to deploying fabric overlay automation.

• **Fabric post-verification**: A tool to verify proper operation of network devices, following fabric overlay automation.
Automating SD-Access with DNA Center

This chapter describes the practical application of SD-Access concepts through the DNA Center platform using the design, policy and provision workflow.

**Network Design**

IT teams in large enterprises often have to manage a large number of distributed sites of varying business functions and natures. For example, a certain enterprise may have retail stores, kiosks, distribution centers, manufacturing sites, and corporate offices. The desire for IT teams in such scenarios often is to simplify their operations through standardizing sites based on their business nature into a network profile. IT teams also need to allow for local teams to manage and customize certain site-specific parameters, such as site-specific logging services, while ensuring other parameters, such as network authentication and policy, are defined consistently across the enterprise.

DNA Center allows for categorizing network infrastructure in terms of sites and also provides granularity to define buildings and floors that closely mirror the physical layout of the organization's network infrastructure. To provide maximum flexibility, DNA Center also allows for a site's hierarchies to be defined.

---

**DIAGRAM DNA Center Network Hierarchy**

- Global
- Site
- Building
- Floor

Settings applied at higher levels will cascade to lower levels by default.

Specific configurations may be customized for lower levels where appropriate.
DNA Center allows for automated configuration on either a global- or per-site basis. DNA Center also supports Zero Touch Provisioning of network infrastructure with Cisco's Plug-n-Play solution to automatically onboard new infrastructure components.

To achieve this, the Design section of the DNA-Center provides the following:

- Network hierarchy creation
- Site-specific network parameters
- Site-based network profiles

**Apply Network Settings**

Settings defined in the Design workflow of DNA Center provide the primary building blocks that will (1) equip the controller to validate network configurations prior to deployment, and (2) minimize further manual entry of these elements during other phases of the automation process. These settings are applied to a network hierarchy as noted above and will serve multiple purposes in subsequent workflow elements.

Settings defined in this workflow include the following:

- **Shared network services configurations** including AAA, DHCP, NTP, and DNS servers.
- **Credentials** with which DNA Center will access network devices.
- **IP address pools** both for client devices and for use in other DNAC workflows, including LAN (Underlay) automation and Fabric Border external connectivity automation.
- **Wireless network configurations** (discussed below in further detail).

**Plan and build wireless network configurations**

Wireless network configurations are fully automated in DNA Center and simply represent another step in the Design/Policy/Provision workflow. Shared elements such as IP address pools, Virtual Networks, and Scalable Group Tags, are integrated into this workflow and do not need to be defined separately.
For features specific to wireless network deployments, including enterprise and guest SSID configurations, Radio Frequency (RF) optimization parameters, and other key features such as Quality of Service (QoS), Fast Lane, and Adaptive 802.11r, configurations are defined and deployed within DNA Center.

**Manage software images**

The Design workflow within DNA Center includes Software Image Management – the capability to automate the management of software images for a variety of network devices, including routers, switches, and Wireless LAN Controllers. This functionality includes multiple validation checks to ensure devices are adequately prepared for an upgrade or downgrade.

**Define policies**

DNA Center enables organizations to create logical network segments and granular group or context-based service policies, which are then automated into prescriptive configurations which get pushed onto the network infrastructure.

There are three primary types of policies that can be automated in the SD-Access fabric as follows:

- **Security**: Access Control policy which dictates who can access what. It has set of rules for cross-group access. For example, permit / deny group-to-group
- **QoS**: Application policy which invokes the QoS service to provision differentiated access to users on the network from an application experience perspective.
- **Copy**: Traffic copy policy which invokes the Traffic Copy service inside DNA Center to configure ERSPAN for monitoring specific traffic flows

**Provision your network**

Once your network design has been defined, automated deployment activities can proceed as follows:
• **Add devices to sites**: This step involves assigning devices from the Inventory to the physical sites created as part of the design workflow. This makes the device ready to accept the site-wide design parameters.

• **Provision network devices (Switches, Routers, WLC and APs)**: This step involves the provision of the configurations based on the design workflow. When the provision step is complete, all the parameters which were set in the design for the site based on Cisco best practices, are provisioned on the device.

### Create Fabric

This step involves selection of fabric edge, fabric border and fabric control plane nodes. Additionally, pre-verification and post-verification checks are provided to verify the state of the devices in the fabric. A fabric is built with the following steps:

1. Add edge nodes to the fabric.
2. Choose your fabric border nodes, At this time the administrator also needs to provide the external and/or transit connectivity parameters. This allows the fabric to connect to the outside networks.
3. Choose your fabric control plane nodes.

### Host Onboarding

Host onboarding allows attachment of end-points to the fabric nodes. The host onboarding workflow will all allow you to authenticate, classify an end-point to a scalable group tag, and associate to a virtual network and IP Pool. Key steps to achieve this are as follows:

1. **Authentication Template selection**: DNA Center provides several predefined Authentication Templates to streamline the process of applying authentication mechanisms to your network. Selection of a template will automatically push the required configurations to the fabric edge.
2. **Virtual Networks and subnet selection for unicast and multicast**: Associate IP address pools to the Virtual Networks (VN).
4. **Static port settings**: This allows settings at port level.
Pre-Verification and Post-Verification checks

Each fabric creation step allows the administrator to do a pre-verification check which ensures that the selected network devices are capable and are correctly configured to accept the fabric provisioning. Likewise, post-verification checks allow the administrator to verify the correct operation of the fabric by highlighting devices which might have reported errors during configuration. This step helps the administrator to find any explicit things that might not be working as expected.

Summary

Once the above tasks are completed to deploy SD-Access fabric, configuration changes to meet evolving use cases can be easily achieved through the DNA Center instead of through manual interaction.
SD-Access Assurance
Assurance

As a network grows and evolves to accommodate new business requirements, complexity grows with it. Complexity is introduced in multiple dimensions: from ensuring that new functionalities can be successfully overlaid on top of existing network designs and architectures, to guaranteeing new features and functionalities co-exist and interoperate successfully with existing ones, to implementing appropriate lifecycle management of the infrastructure without disrupting the business.

In addition, as the role of the network becomes more prominent, any outage or degradation in the network performance is proportionally disruptive to the business. As a result, IT is constantly under pressure to ensure optimal connectivity and user experience for the applications, no matter where the user is connecting from, which device he/she is using, or which application he/she is trying to access.

In essence, IT is faced with the following challenges:

- **Reactive troubleshooting**: IT is often made aware of an incident after it occurs and must troubleshoot it reactively.
- **Disparate tools**: Enterprises have a plethora of tools which introduce complexity because each tool only provides a subset of the required functionality.
- **Lack of insights**: Today's tools often provide data that isn't correlated, and as a result, are unable to drive actionable insights.

Cisco's Digital Network Architecture (DNA) defines **Assurance** as the ability to quantify network availability and risk. This includes the following elements:

- **Telemetry**: Collection of operational data from a wide variety of network sources.
- **Key Performance Indicators (KPIs)**: Well-defined metrics that indicate a condition such as link status, which may be measured as a binary value (up/down) or a changing value (such as CPU utilization).
- **Issues**: Negative conditions with an associated severity derived from correlated KPIs.
• **Trends**: A historical view of a certain KPI. This may often be used as a forward indicator of a future state.

• **Health Scores**: Quantified health of clients, applications, or network devices based on KPIs of the operational state of the IT infrastructure.

• **Insights**: Actionable next steps corresponding to an issue or trend.

• **Reporting**: A summary readout of various aspects of network management or operations such as Inventory, Issues, Compliance, etc.

**What is Assurance in the context of Cisco SD-Access?**

Cisco SD-Access Assurance provides analytics and insights for two main categories: network underlay (non-fabric) and fabric overlay.

Analytics provided for the **Network Underlay** include the following:

- Network – traditional (non-fabric) LAN, WLAN and WAN protocols and tables
- Device – switch, router, wireless software and hardware (CPU, memory, temperature, etc.)
- Client – traditional (non-fabric) wired and wireless client status and statistics
- Application – traditional (non-fabric) wired and wireless flow status, statistics, and performance

Analytics provided for the **Fabric Overlay** include the following:

- Fabric reachability – connectivity checks between all the fabric nodes
- Fabric device – fabric nodes mapping entries, protocols, and performance
- Fabric clients – client onboarding and shared services (DHCP, DNS, AAA, RADIUS)
- Group-based policies – ISE (pxGrid, AAA) and border and edge node policy entries
Telemetry

The data analytics platform within DNA Center collects data from a number of sources to provide insights related to the network, including its clients and applications. Contextual data is collected from the network infrastructure layer (routers, switches, WLCs etc.) and various other systems connected to the network (Cisco ISE, AppDynamics, ITSM, IPAM etc.). This data is correlated within the data analytics platform to provide actionable insights, with root cause analysis and impact assessments related to network, client, and application health.

The below content will outline the primary topics around telemetry as follows:

- **Telemetry collection mechanisms**: what are the key methods for ingesting data from diverse network devices?
- **Telemetry Quotient**: how does one achieve useful visibility into the network by collecting the right data and doing so in the best manner?
- **Proactive telemetry with network sensors**: how can network performance and stability concerns be detected at the network edge?

**Telemetry Collection Mechanisms**

Telemetry data is collected from the network infrastructure using various mechanisms, based upon the capability of the network device or the software image running on the device. Some of the collection mechanisms include:

**Streaming telemetry** enables network devices to send near real-time telemetry information to DNA Center, reducing delay in data collection. Some of the other benefits of streaming telemetry include:

- Low and quantifiable CPU overhead
- Optimized data export (KPI, events)
- Event-driven notifications
Assurance also ingests **standard telemetry** mechanisms such as **SNMP**, **SNMP Traps**, **syslog** messages, **Netflow** export data for application flow-related information, and operational data collected using the CLI show commands.

DNA Center will collect contextual data from other connected systems such as Cisco ISE, AppDynamics, ITSM and IPAM systems.

**Telemetry Collection with Network Sensors**

In order to identify issues in the network, there is a need to **proactively** test the quality of the network connection by assessing multiple elements end-to-end, including the following:

- **Onboarding**: How long does it take for the client to get an IP address?
- **Reachability**: Are important network services (such as DHCP, DNS and AAA servers) reachable and stable?
- **Performance**: How well are key network applications performing?

Assurance leverages wireless sensors to proactively test the network, providing a critical dimension to performance monitoring. DNA Center's Sensor Management workflow can leverage either dedicated Access Points or can selectively convert Access Point radios into Sensor Mode using Flexible Radio Assignment (FRA). Scheduled tests from these sensors will then feed corresponding telemetry back to DNA Center.

**Telemetry Quotient**

With its **Telemetry Quotient** feature, Assurance offers administrators the capability to (1) identify where they may be missing valuable visibility into their network, and (2) provision rich telemetry configurations as appropriate, based on a number of factors such as device model and software version.
Health and Insights

Wearing the IT operator’s hat for a moment, imagine receiving a ticket for a network connectivity issue. The ticket description of the problem is "user anna_rossi@acme.it claims that the wireless network is too slow". This sounds familiar. So, where to start?

What if there was a single dashboard to present a summary of all network- and client-related information, for wired and wireless access media, with an integrated timeline? The page would not only give a summary of all clients in the network but it would also allow for a search for a specific username or MAC address, and would display user-specific information.

Overall Health

The concept of "health" in DNA Center goes far beyond individual Key Performance Indicator (KPI) views. While KPIs themselves are of course important, they support a broader goal of delivering the most important and actionable information in the shortest amount of time – in some cases even before a "condition" has become a "problem" that is impacting users and services.

DNA Center Assurance provides correlated, actionable insights based on a wide variety of telemetry data ingested from sources throughout the network. The highest level of these insights is presented as an **Overall Health** dashboard that answers the following top-level questions:

- **How healthy is my network?** If components of my network are unhealthy, at a high level, which infrastructure categories, in particular, are unhealthy – Core, Distribution, Access, or Wireless?

- **How healthy are my clients?** If there are unhealthy clients present, are they wired (and thus RF concerns are excluded) or are they wireless?
The overall health dashboard (shown in the diagram below) answers these questions in three primary views, with a fourth "Issues" view for additional drill-down capability into any highly critical conditions that require immediate attention. Each of these views is described further below.

- **Map and Topology Overall Health**: leverages the network hierarchy as defined previously in the Design workflow and reflects high-level network and client health information.

- **Global Network Health**: reflects how much of the network is operating at a level that is considered to be "healthy" – that is to say, what overall percentage of the network devices are operating at or above a score of 8 (on a scale of 1 to 10). In this view, the global network health score is further broken down into its key components – Core, Access, Distribution, and Wireless – based on device roles as defined elsewhere in DNA Center’s inventory or topology views.

- **Global Client Health**: indicates the percentage of your network’s clients which are currently operating at a healthy level of 8 or above on a scale of 1 to 10. The summary score reflects both wired and wireless clients together. The global client health score is further broken down into wired and wireless components for quick comparison.

- **Top Global Issues**: indicates high-impact issues such as routing protocol adjacency failures. Issues highlighted in these dashboards drill down directly to a detailed view of relevant data and any suggested actions that may be taken in order to quickly focus on the real root cause concern.
Network Health

The Network Health view summarizes Assurance information at the network device level in three main views:

- **Network Map and Topology**: shows the geographical map or topology view with sites and their associated health scores.

- **Network Health Summary**: reflects the health of network elements being monitored across all sites or domains. This score is further broken down into its key components – Core, Access, Distribution, and Wireless.

- **Fabric Network Health**: indicates the health of constituent physical sites of the fabric, including the network devices that play certain functions in the fabric such as control plane nodes, fabric borders, etc. and the health of the clients and application traffic that the fabric supports.

SD-Access Fabric Health

SD-Access Fabric Health Scores fall into the following three categories:

- **System Health**: Considers metrics such as CPU and memory utilization for switches, routers, APs, and Wireless LAN Controllers.

- **Data Plane Connectivity**: Considers metrics such as link errors and uplink availability status with additional RF-related information for wireless networks.

- **Control Plane Connectivity**: Considers metrics such as connectivity or reachability to the fabric control plane node.
Fabric Insights

- **Control Plane Insights**: Assurance provides insights into the fabric underlay and overlay control planes in a correlated manner by checking for reachability (link down, adjacencies flapping), measuring control plane response times (latency), and validating device configurations (MTU mismatches) that may lead to network problems.

- **Data Plane Insights**: Assurance leverages IPSLA to proactively generate probes, both in the underlay and overlay from fabric border towards shared services in order to detect problems. It also leverages Path-trace functionality to provide additional context.

- **Policy Plane Insights**: Assurance gives visibility into the policy instantiations on network elements, such as whether SGACLs have failed to download or failed to instantiate due to a lack of TCAM resources.

- **Device Insights**: Assurance monitors many individual resources such as CPU, memory, temperature, environment, fan, line cards, POE power, and TCAM tables of the physical network devices, and can provide trending capabilities to help avoid issues from happening in the fabric.
Client Health

The Assurance Client Health page provides an easy-to-use single dashboard for monitoring a summary of client analytics for the entire network, including the following:

- **Onboarding time**: the time it takes for the clients to authenticate and get an IP address.
- **Connection quality**: measured as Connectivity RSSI for wireless, and physical link for wired.
- **Client operating system** for wired and wireless.

These insights are key to monitoring and troubleshooting the users' actual experience, and most of the time, they help the IT operator to respond effectively to any problem that has already occurred.

From the example above, the IT operator can now search for "anna_rossi" in the main Client Health page (or even in the main Assurance page) and can double-click into specific user health information through a dedicated page called Client 360 view that provides basic but important information such as a summary issues, client health score over time, and user onboarding path.

For a wireless user, the onboarding chart reflects critical information such as the Access Point and radio the user is connected to, the next hop switch, and the WLC with which she is associated. This is represented in the below diagram.
**Client Score Timeline**

The Client Score Timeline provides a visual and intuitive "DVR" view into the history of a client's experience, including important factors such as the onboarding time and the connection quality.

The timeline provides a retrospective view of client concerns and enables the IT operator to troubleshoot issues even if they are unreproducible. In the above example, for instance, it would be clear that anna_rossi experienced a slow network because her device, despite being a dual-band client, was preferring the 2.4GHz radio instead of 5Ghz.

**Advanced RF Metrics**

Specifically for wireless users, Assurance presents key RF-related KPIs to assess the wireless experience of the client; the information is represented in graphs that show important values such as Received Signal Strength Indicator (RSSI), Signal Noise Ratio (SNR) and data rate over time.

**Wi-Fi Analytics for iOS**

It has traditionally been a difficult task to determine the actual experience of end-user devices on WiFi networks. Thanks to a partnership between Cisco and Apple, as of Apple iOS 11, DNA Center Assurance is able to ingest this valuable feedback from supported Apple devices, answering questions such as these:

- What are some relevant details around the types of Apple devices accessing the network?
- How does the device itself "see" the network? For instance, which Access Points are heard better than others?
- What was the device's most recent reason for disconnecting?

This capability is unique to Cisco and is helpful, not only in identifying potential short-term issues and concerns but also in trending client device behaviors over time.
Reporting

In future releases, DNA Center will provide both pre-defined and customizable reporting capabilities to help plan capacity, detect overall baselines and pattern changes for client and infrastructure devices, and provide views into operational activities such as software upgrades and provisioning failures.

DNA Center Assurance reporting will include the following features:

- Run on-demand or as scheduled for one-time or recurring execution
- Export reports in multiple formats
- Automatically sent to recipients via email
- Target one site or across all sites
- API-based interfaces to allow for integration to other systems.

Among other items, reports will include inventory, client, audit, and infrastructure views for both fabric and non-fabric topologies.
Integration with Partner Ecosystems
Introduction

The value of SD-Access in terms of enhancing IT agility and efficiency is further augmented through ecosystem integrations with other Cisco and non-Cisco solutions and products. These integrations help customers manage the entire enterprise environment, including the network infrastructure as a single orchestrated entity, enabling faster introduction of new services and helping focus on business outcomes.

These integrations are built using the open northbound DNA Center APIs that expose a rich set of intent-driven business flows along with data-as-a-service. DNA Center provides integration capabilities and a development environment that can be leveraged by Independent Software Vendors (ISV) partners, customers, and ecosystem partners. Examples include integrations with IT Service Management (ITSM), IP Address Management (IPAM), and others such as:

- API catalog and documentation
- Runtime Monitoring and Analytics
- API Lifecycle Management
- Sample code and script generation capability

![DNA Center Platform Ecosystem Diagram](image-url)
APIs & Programmability

APIs in the SD-Access solution fall into the following three categories:

- **Device APIs** for direct access to configuration and operational functionality on individual network devices
- **DNA Center APIs** for network-wide automation and orchestration
- **Identity Services Engine (ISE) APIs** for rich contextual data about user and device access

These three categories are explored in further detail below.

**Device APIs**

Network infrastructure devices based on IOS-XE provide APIs that are based on IETF and OpenConfig YANG Models as well as Cisco native models and are exposed via NetConf, RestConf and gRPC interfaces. These APIs support both configuration automation and operational models. Newer IOS-XE devices (Catalyst 9000, ASR, ISR etc) additionally support Streaming Telemetry, which allows analytics solutions to subscribe to low-latency datastreams based on YANG data-models for real-time data analytics at scale.

**DNA Center APIs**

DNA Center provides REST APIs for network-wide automation and orchestration. This helps provide an abstracted view of the network such that customers can drive network automation at scale. Additionally, DNA Center will provide REST APIs to expose operational data present in Client 360, Device 360 and Application 360 views along with issues, trends and insights. This enables external entities to consume and create business-relevant, data-driven workflows.
Identity Services Engine APIs

Cisco Identity Services Engine (ISE) APIs expose contextual information about network behavior, including User and Device access policies, authentication and authorization events, and more. These APIs also allow for policy-related configuration automation, such as enabling external systems to trigger changes of authorization for users and endpoints for rapid threat containment, and provides a platform-exchange grid (pxGrid) for rich integration with more than 80 ecosystem partner integrations.
Ecosystem Integrations

Customers are able to derive enhanced value and functionality from the SD-Access architecture through open northbound REST APIs from DNA Center and integrations with other solutions that are part of the DNA ecosystem. The ecosystem integrations span various categories of solutions such as IP Address Management, IT Service Management, Public Cloud, external SDN Orchestrators, Security Analytics & Operations, Security Infrastructure such as firewalls, and more.

Some of the key capabilities that are achieved as a result of these integrations include:

- **Improved operations and security**: Through orchestration between external systems and SD-Access, customers can programatically define and deploy closed-loop systems that take insights and state information from the network, enrich it with external data and functionalities, and feed a response action back to the network. This helps customers operate multiple systems with independent automation and management platforms as a single orchestrated entity, thereby accelerating IT agility, efficiency and improving security posture.

- **Simplified best-of-breed deployments**: In an increasingly complex yet innovative world, customers are often looking for best-of-breed tools to incorporate into their IT environments which address key functionalities desired by the customer or end-user. Open APIs and validated interoperability ensure that an end-to-end orchestrated environment can be easily deployed.

- **Enhanced value from technology investments**: For customers who have already adopted and standardized on certain Cisco or non-Cisco solutions, the ecosystem integrations help ensure that customers gain maximum value from existing investment while adopting SD-Access.

The capabilities for each of the solution and vendor integrations is evolving rapidly. Below is a sample of the various integrated technology partners currently in development, and the joint functionalities with SD-Access.
**IP Address Management (IPAM)**

SD-Access offers a validated integration with leading IPAM solutions such as InfoBlox and Bluecat through IPAM-API integration. This enables the customer to use IP Address Pools defined in their IPAM solution to be imported into DNA Center for use in SD-Access, and also IP address pools defined in DNA Center to be available in IPAM.

**Cisco Network Services Orchestrator**

Some large enterprise customers have standardized on Cisco Network Services Orchestrator (NSO) as their network orchestration solution, to have a single way to automate management of their WAN, data center and campus deployments using the NetConf/RestConf interfaces of NSO and the infrastructure. SD-Access deployments can be orchestrated by Cisco NSO through APIs exposed from DNA Center, and used by Cisco NSO.

The key benefits of SD-Access integration with Network Orchestrators include:

- Agile service management: reduces time to market for deploying new services.
- Best-in-industry multi-vendor support.

**Firewalls**

Integration of Cisco's ASA with Cisco SD-Access enables the firewalls to have full access to context information, including the security context of the endpoint's group classification. This enables simplified policy administration and monitoring of traffic through firewalls, such as ASA Firewalls and Firepower Threat Defense Firewalls, in a manner that is consistent with the policy model in DNA Center. This integration is also available from non-Cisco firewalls such as CheckPoint.

**Security Analytics**

Integrations between Security Analytics solutions such as StealthWatch and SD-Access empower network and security teams to accelerate incident response. Through the Rapid Threat Containment capabilities of ISE as part of Cisco SD-Access, hosts identified as being compromised or exhibiting suspect behavior through StealthWatch can be easily quarantined or blocked on the network.
To summarize, some of the key benefits of SD-Access integration with advanced Security Analytics solutions include:

- Proactively identifying and reporting potential security threats
- Segmenting or isolating the network to contain threats
- Automating security and network operations
Summary, Next Steps, and References
Summary

A lot of ground has been covered to arrive at this point. The challenges involved with today’s network deployments have been examined, how SD-Access helps to address those challenges, and how it assists organizations to move into a digitized future, have also been considered.

The use of SD-Access drives multiple benefits for an organization:

**Greater speed and agility**: SD-Access allows an organization to move faster and more nimbly – allowing for more rapid and seamless deployment of new network innovations that support business requirements and generate more successful outcomes.

**Greater efficiency, deeper insights**: SD-Access allows an organization to save money, by allowing for significantly more rapid and secure network deployment, driving greater efficiencies in network operation, and by providing insights into the ways users are leveraging the network and the operation of the applications that are in use.

**Reduction of Risk**: SD-Access allows an organization to provide integrated security as an inherent property of the SD-Access fabric, lowering the attack surface of the network and providing granular user/device/application access controls, allowing an organization to rapidly roll out and maintain an inherently secure and flexible infrastructure.

All of this is made possible by the key elements within SD-Access fabric that we have examined: Automation, Policy and Assurance, all enabled by DNA Center. SD-Access provides a substantially more powerful and flexible way to deploy enterprise networks that are at the same time simpler to design, deploy, and operate.

SD-Access gives IT time back by dramatically reducing the time it takes to manage and secure a network. It also improves the overall end-user experience.
## Benefits of SD-Access

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Provisioning</td>
<td>67%</td>
<td>Reduction in network provisioning costs</td>
</tr>
<tr>
<td>Threat Defence</td>
<td>48%</td>
<td>Reduction in cost impact of a security breach</td>
</tr>
<tr>
<td>Monitoring and Troubleshooting</td>
<td>80%</td>
<td>Reduction in cost impact of a security breach</td>
</tr>
<tr>
<td>End User Experience</td>
<td>94%</td>
<td>Reduction in costs to optimize policies</td>
</tr>
</tbody>
</table>

Summary, Next Steps, and References
Next Steps

So now that SD-Access and its benefits have been understood, what are the next steps a network administrator can take? More importantly, how can an organization begin its journey towards a software-defined future?

SD-Access offers several value propositions for common challenges encountered in traditional enterprise networking, based on evolving trends around mobility, enterprise IoT and cloud; and providing for an agile, secure enterprise networking architecture. SD-Access can be deployed on existing networks and for new infrastructure projects.

**Identify Key Objectives and Use-Cases**
In order to migrate an existing network to an SD-Access architecture, it is worthwhile to start with identifying the key objectives or use-cases for the network environment, including anticipated and upcoming needs that may need to be addressed. Based on the stated key objectives of the network architecture and the content covered in this book, one could map how the capabilities offered by SD-Access can be applied to the use-cases of the organization.

**Assess Infrastructure Readiness**
Once the SD-Access deployment use-case objectives have been defined, the next step is to identify parts of the network infrastructure that will be migrated to the SD-Access architecture to achieve project objectives. This includes planning for the deployment of DNA Center and Cisco Identity Services Engine (ISE) based on use-case needs. It is also advisable to consider the hardware and software compatibility of the network infrastructure under consideration to meet the solution deployment needs.

**Define Policy Objectives**
Moving to SD-Access often entails discussing policy objectives for the environment with the appropriate stakeholders, based on business requirements. This is an important consideration since the policies in SD-Access are applied in terms of business functions on a network-wide basis versus traditional methods. As a result, design of group structures and key criteria to map the organization's endpoints can greatly facilitate future policy definition and automation. Once appropriate policy
objectives are defined, organizations can rapidly start to realize the benefits of centralized policy automation with SD-Access.

It is recommended that organizations start with a coarse grouping structure, such as Employees versus Partners, before moving on to more granular classifications such as Finance Employee versus HR Employee. This ensures that the number of Scalable Groups can grow alongside the customer’s operational familiarity with the SD-Access policy model.

**Plan & Execute the Migration**

Some customers, especially when trying to incorporate SD-Access into their brownfield projects, may choose to go down the path of installing a new parallel network infrastructure that is exclusively SD-Access-enabled while keeping the older network in place. Others will perform a phased migration by selecting a specific segment or segments of their network as initial migration targets. In either case, it is recommended that customers start with a limited area of deployment and pilot SD-Access, familiarize themselves with the operations and technology, and then over time, expand the deployment and use-cases.
References

Additional sites which offer more detailed information on Software-Defined Access include:

https://www.cisco.com/go/sda - provides an overview and additional information on all components and aspects of SD-Access: Automation, Assurance, supported platforms, customer references and testimonials, and a wealth of the most up-to-date information on SD-Access deployments and capabilities.


https://www.cisco.com/c/en/us/solutions/design-zone.html - references the Software-Defined Access guide. This is a Cisco Validated Design (CVD) document covering SD-Access design options, operational capabilities, and recommendations for deployment. It provides direct insight into the best practices for the design, operation, and use of SD-Access in customer network deployments.

Cisco Live 365 Sessions: https://www.ciscolive.com/global/on-demand-library/?#/ (search for the session IDs shown below):

- Cisco SD-Access – A Look Under the Hood – BRKCRS-2810
- Cisco SD-Access – External Connectivity – BRKCRS-2811
- Cisco SD-Access – Migration – BRKCRS-2812
- Cisco SD-Access – Monitoring and Troubleshooting – BRKCRS-2813
- Cisco SD-Access – Assurance – BRKCRS-2814
- Cisco SD-Access – Policy – BRKCRS-3811
- Cisco SD-Access – Wireless Integration – BRKEWN-2020
- Cisco SD-Access – DC Integration – BRKDCN-2489

Cisco SD-Access YouTube channel: www.youtube.com/user/cisco (search for “SD-Access”)
Acronyms

AAA – Authentication, Authorization, and Accounting

ACI – Application-Centric Infrastructure

ACL – Access Control List

AD – Active Directory

AP – Access Point

APIC – Application Policy Infrastructure Controller

BGP – Border Gateway Protocol

CAPWAP – Control and Provisioning of Wireless Access Points

CDB – Cisco Digital Building

CDP – Cisco Discovery Protocol

CLI – Command Line Interface

CP – Control Plane

CPP – Cloud Policy Platform

DHCP – Dynamic Host Configuration Protocol

DMVPN – Dynamic Multi-point VPN

DNA – Digital Network Architecture
DNAC – DNA Center
DNS – Domain Name System
EPG – Endpoint Group
ERSPAN – Encapsulated Remote Switch Port Analyzer
GUI – Graphical User Interface
HIPAA – Health Insurance Portability and Accountability Act
HSRP – Hot Standby Routing Protocol
IE – Industrial Ethernet
IP – Internet Protocol
IS-IS – Intermediate System to Intermediate System
ISE – Identity Services Engine
IT – Information Technology
LAN – Local Area Network
LISP – Locator/Identity Separation Protocol
MAC – Media Access Control
MPLS – Multi-protocol Label Switching
NETCONF – Network Configuration Protocol
OSPF – Open Shortest Path First
OT – Operational Technology

PCI – Payment Card Industry

PIM – Protocol Independent Multicast

PIM-ASM – PIM Any Source Multicast

PIM-SSM – PIM Source Specific Multicast

PXGRID – Platform Exchange Grid

SD-Access – Software-Defined Access

SGACL – Scalable Group Access Control List

SGT – Scalable Group Tag

SIEM– Security information and event manager

SNMP – Simple Network Management Protocol

SPAN – Switch Port Analyzer

STP– Spanning Tree Protocol

SXP – SGT Exchange Protocol

TLV – Type Length Value

VN – Virtual Network

VNI – Virtual Network Instance

VPN– Virtual Private Network
VRF – Virtual Routing and Forwarding

VRRP – Virtual Router Redundancy Protocol

VXLAN – Virtual Extensible Local Area Network

WLC – Wireless LAN Controller