CISILION

CISCO

Cisco Software-Defined Access

Introducing an entirely new era in networking.

What if you could give time back to IT? Provide network access in minutes for any user or device to any application-without compromise?

Software-Defined Access (SD-Access) is the industry's first intent-based networking solution for the Enterprise built on the principles of Cisco's Digital Network Architecture (Cisco DNA). SD-Access provides automated end-to-end segmentation to separate user, device and application traffic without redesigning the network. SD-Access automates user access policy so organizations can make sure the right policies are established for any user or device with 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.

Benefits

- Consistent management of wired and wireless network provisioning and policy

- Automated network segmentation and group-based policy

- Contextual insights for fast issue resolution and capacity planning

- Open and programmable interfaces for integration with third-party solutions

SD-Access solution overview

Cisco SD-Access enables IT transformation by improving operational effectiveness, enhancing the workforce experience and increasing security and compliance. Building this next-generation solution involved some key foundational elements, including:

· Controller-based orchestrator

· Network fabric

· Programmable switches

Controller-based networking: Traditional networking focuses on per-device management, which takes time and creates many complexities. This approach is prone to human errors. SD-Access uses a modern controller architecture to drive business intent into the orchestration and operation of network elements. This includes the day-0 configuration of devices and policies associated with users, devices and endpoints as they connect to the network. The controller provides a network abstraction layer to arbitrate the specifics of various network elements. Additionally, the Cisco DNA Center controller exposes northbound Representational State Transfer (REST)-based APIs to facilitate third-party or in-house development of meaningful services on the network.

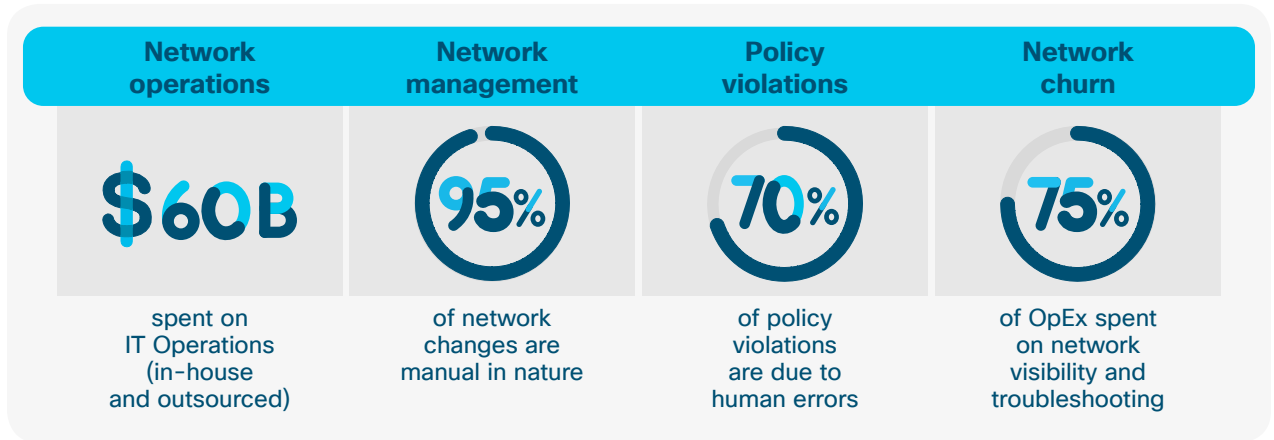Figure 1. SD-Access overview
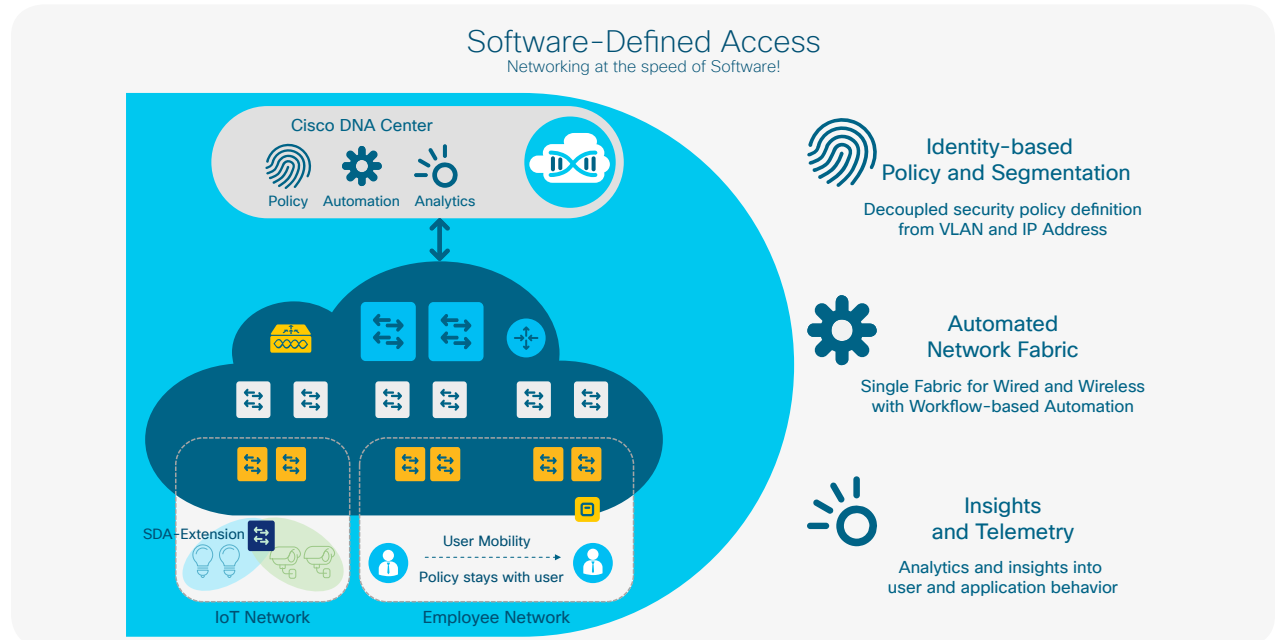
Why SD-Access?

There are many challenges today in managing the network because of manual configuration and fragmented tool offerings.

Manual operations are slow and error-prone and these issues are exacerbated due to the constantly changing environment with more users, devices and applications. With the growth of users and different devices types coming into the network, configuring user credentials and maintaining a consistent policy across the network is more complex. If your policy is not consistent, there is the added complexity of maintaining separate policies between wired and wireless. As users move around the network, locating the users and troubleshooting issues also become more difficult. The bottom line is that the networks of today do not address today's network needs.

CISILION

Network fabric: With a controller element in place, you can consider building the network in logical blocks called fabrics. The SD-Access Fabric leverages Virtual Network Overlays in order to support mobility, segmentation and programmability at very large scale. The Virtual Network Overlay leverages a control plane to maintain the mapping of end-points to their network location up to date as end-points move around the network. Separation of the control plane from the forwarding plane reduces complexity, improves scale and convergence over traditional networking techniques. The SD-Access Fabric enables several key capabilities, such as the host mobility regardless of volume of moves and size of the network, Layer 2 and Layer 3 segmentation, and wireless integration. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization and steering for optimum performance and operational effectiveness.

Modern device software stack:
To build a modern infrastructure, Cisco is equipping existing and future switches with advanced capabilities to enable full lifecycle management while being open, standards-based and extensible. These key technologies include (1) automated device provisioning, incorporating well-known functions such as zero-touch provisioning, Plug and Play and Preboot Execution Environment; (2) open API interface; (3) granular visibility, using telemetry capabilities such as NetFlow; and (4) seamless software upgrades with live software patching.

Network operations	Network management	Policy violations	Network churn
$60B	**95%**	**70%**	**75%**
spent on IT Operations (in-house and outsourced)	of network changes are manual in nature	of policy violations are due to human errors	of OpEx spent on network visibility and troubleshooting

These challenges are deeply rooted within network deployment and operations as noted below:

Network deployment

- Setup or deployment of a single network switch can take several hours due to scheduling requirements and the need to work with different infrastructure groups. In some cases, deploying a batch of switches can take several weeks.

- Security is a critical component of managing modern networks. Organizations need to appropriately protect resources and make changes efficiently in response to real-time needs. Tracking VLANs, Access Control Lists (ACLs) and IP addresses to ensure optimal policy and security compliance can be challenging.

- Disparate networks are common in many organizations, as different systems are managed by different departments. The main IT network is typically operated separately from building management systems, security systems and other production systems. This leads to duplication of network hardware procurement and inconsistency in management practices.

Ordering information

Please refer to the SD-Access ordering guide for detailed information.

Network operations

- **Limited change management:**

  One of the standard operational activities in running a network is to upgrade software and configurations periodically. Whenever such a change is required on a typical network, the sheer logistics mean the task could take over 6 months.

- **Productivity:**

  Every business strives to provide a high-quality communication experience to optimize employee productivity. However, this effort has been difficult and time-consuming with current models. Experience has shown that changes in quality of service can take several months to plan and implement, while lack of implementation causes performance issues in business-critical applications.

- **Slow resolution of issues:**

  The significant size and complexity of networks under the current network management paradigm mean that whenever a failure occurs, pinpointing and resolving the issue can take a great deal of effort and time. There is also a lot of data that is being collected but not properly correlated to understand the various contexts of network and user behaviors.

Solution components

The core components that make up the SD-Access solution are:

- Cisco DNA Center
- Cisco Identity Services Engine (ISE)
- Network platforms

CISILION

Key features

See Table 1 for a list of the key features of SD-Access 1.x (New updates in 1.2.x)

Table 1. SD-Access 1.x (update 1.2.8) Key Features

Feature	Description
Fabric infrastructure	• Automated external connectivity handoff using Virtual Routing and Forwarding Lite (VRF-Lite), and Border Gateway Protocol (BGP) • Border automation with existing BGP configurations • Fabric readiness and compliance validations • SD-Access for Distributed Campus • SD-Extension for IoT (beta) • Support for an internal border for DC connectivity • Connectivity between hosts in the fabric and an external Layer 2 domain • Fabric-in-a-box wherein a device can be the edge, border and control nodes simultaneously • Support for Broadcast, Link-local multicast traffic in the overlay • Ability to assign a fabric edge switchport as a trunk to facilitate server connectivity • Support for Native Multicast enabled. • Catalyst 9200 Series Switches as Fabric Edge (New in update 1.2.8) • Automatic checks on a device for fabric-readiness and fabric-compliance (New in update 1.2.8) • Support for Layer 2 Border Handoff on Catalyst 6000 Series Switches (New in update 1.2.8) • Enhancements in Underlay LAN Automation (New in update 1.2.8) • Support for management interface as the source interface for reachability to AAA servers (New in update 1.2.8) • API support for adding and deleting borders (New in update 1.2.8)
Fabric control plane	• Demand-based overlays with LISP-based control plane • Control plane co-located with fabric border or standalone • Resiliency with support for multiple LISP control plane nodes

Feature	Description

Fabric Assurance	• KPIs, 360 views for Client, AP, WLC, and Switch
	  - Underlay & Overlay Correlation
	  - Device Health: Fabric Border and Edge; CPU, Memory, Temperature, Linecards, Modules, Stacking, PoE power, TCAM
	  - Dataplane Connectivity: Reachability to Fabric Border, Edge, Control Plane, and DHCP, DNS, AAA
	  - Policy: Fabric Border and Edge Policy, ISE/PxGrid Connectivity
	  - Client Onboarding: Client/Device DHCP & DNS, Client authentication & authorization
	  - Traffic Visualization and Network Service Assurance with LiveNX from LiveAction

Security	• Host Onboarding Enhancement – IBNS 2.0

Segmentation	• Network segmentation and Group-based Segmentation
	• Group assignment capabilities using multiple authorization methods with Identity Services Engine integration
	  - Static: IP to Group Mapping, subnet to Group Mapping, Port to group mapping
	  - Dynamic
	    - MAC address based
	    - Passive identity (Active Directory)
	    - 802.1X based (open, closed)
	    - WebAuth
	    - Device Profiling
	    - Device Posture assessment
	• Default permit for all intra-VN communications between Groups
	  - Option to define custom deny between groups within a VN
	• Default deny for all inter-VN communications between Groups
	  - Option to define custom permit between groups at firewall
	• Add/remove/modify Virtual Networks and Group-based Policies, independent of network devices or location of user
	• Ability to have the same VLAN name across sites for a common policy (New in update 1.2.5)

Feature	Description

Fabric Wireless	• Enterprise wireless support
	• VXLAN support at access point
	• Distributed data plane for higher wireless performance
	• Seamless roaming within the fabric site
	• Wireless Guest with ISE (CWA)
	• Wireless Guest Support on Separate Guest Border/Control Plane and Wireless Guest Support as separate VN on Enterprise Border/Control Plane
	• Same SSID for Traditional and Fabric on same WLC (Mixed Mode)
	• WLC SSO
	• Wireless Multicast
	• Enable Fabric for brownfield WLC
	• Advanced RF profiles (Simplified RF provisioning with default RF profile)
	• Advanced SSID (Band-select, Hidden-SSID, Band for SSID, per site PSK support)
	• Zero Touch Provisioning (ZTP) for Access Point
	• Common WLC for Fabric/Non-Fabric per Site
	• OTT Guest support using an Anchor WLC
	• Greenfield support for embedded wireless on Catalyst 9300 Series Switches in two topologies (New in update 1.2.8):
	  – Co-located Border and Control Plane
	  – Fabric-in-a-box

Fabric security	• Control plane protection against Distributed Denial of Service (DDoS) attacks • Routing Locator (RLOC) authentication with control plane • RLOC source address spoofing prevention
Management	See the list of management features in [Cisco DNA Center 1.2](#)
Technology partners	• IPAM-Infoblox, Bluecat • Integrated threat defense-Cisco Stealthwatch® • Firewalls-Cisco ASA, Cisco Firepower® Threat Defense • Visibility-LiveAction

For more information on all the key features of SD-Access 1.x, refer the [Cisco DNA Center release notes](#).

SD-Access 1.x Hardware and Software Compatibility Matrix is available at the following location: https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html.

CISILION

SD-Access use cases

Building on the foundation of industry-leading capabilities, SD-Access can now deliver key business-driven use cases that truly realize the promise of a digital enterprise while reducing the total cost of ownership (Table 2).

Table 2. SD-Access use cases

Use case	Details	Benefits
Security and segmentation	· Onboard users with 802.1X, Active Directory, and static authentication · Group users with Cisco TrustSec (security group tags) · Automate VRF configuration (lines of business, departments, etc.) · Traffic analysis using AVC and NetFlow is further enhanced using Encrypted Traffic Analytics (ETA)	· Reduced time to provision network segmentation and user groups · Foundation to enforce network security policies · Ability to detect and intercept threats at line rate (not samples) from the center to the last mile, including all devices on the network edge
User mobility	· Single point of definition for wired and wireless users · Seamless roaming for wireless · Distributed data plane for wireless access · Simplified guest provisioning for wireless	· Management of wired and wireless networks and users from a single interface (Cisco DNA Center) · Ability to offload wireless data path to network switches (reduce load on controller) · Scalable fabric-enabled wireless with seamless roaming across campus
Guest access	· Define specific groups for guest users · Create policy for guest users' resource access (such as Internet access)	· Simplified policy provisioning · Time savings when provisioning policies
IoT integration	· Segment and group IoT devices · Define policies for IoT group access and management · Device profiling with flexible authentication options	· Simplify deployment of IoT devices · Reduce network attack surface with device segmentation

© 2019 Cisco and/or its affiliates. All rights reserved.

Use case	Details	Benefits
Monitoring and troubleshooting	• Multiple data points on network behavior (syslog, stats, etc.) • Contextual data available per user and device	• Significantly reduce troubleshooting time • Use rich context and analytics for decision making
Cloud/data center integration	• Identity federation allows exchange of identity between campus and data center policy controllers	• Administrator can define user-to-application access policy from a single interface • End-to-end policy management for the enterprise • Identity-based policy enforcement for optimized ACL utilization • Flexibility when enforcing policy at campus or data center
Branch integration	• Create a single fabric across multiple regional branch locations • Use Cisco routers as fabric border nodes	• Simplified provisioning and management of branch locations • Enterprisewide policy provisioning and enforcement

Services

Accelerate your journey to a digital-ready network with Cisco Software-Defined Access services.

Cisco Services provides expert guidance to help you achieve a streamlined operational model across wired and wireless environments at a lower cost. With proven experience, best practices, and innovative tools, Cisco Services works with you to easily manage, scale, and secure your SD-Access solution. By choosing from a comprehensive lifecycle of services-including advisory, implementation, optimization, and technical services-you can move to a secure and automated unified network with ease and confidence. Learn more.

- Develop an SD-Access architectural strategy and roadmap that aligns to business needs
- Migrate with high performance, security, and reliability
- Achieve operational excellence with optimization
- Maintain reliability and accelerate the ROI of your SD-Access solution
- Reduce disruption with proactive monitoring and management
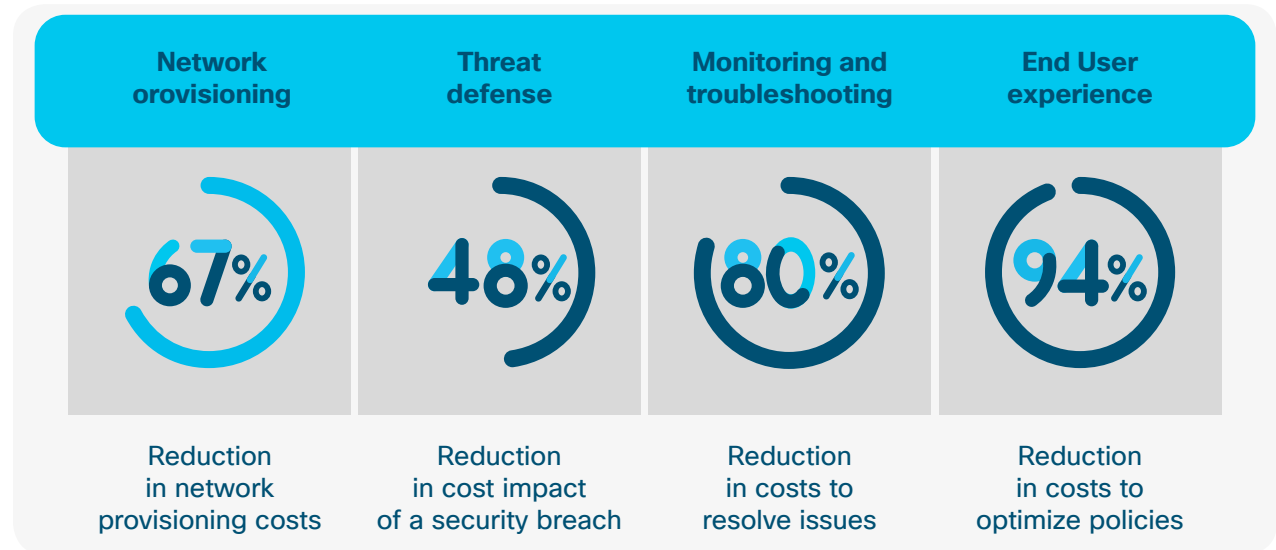- Equip your IT staff with knowledge and training

CISILION

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Giving IT time back with SD-Access

SD-Access gives IT time back by dramatically reducing the time it takes to manage and secure your network and improving the overall end-user experience.

Network orovisioning	Threat defense	Monitoring and troubleshooting	End User experience
67%	**48%**	**80%**	**94%**
Reduction in network provisioning costs	Reduction in cost impact of a security breach	Reduction in costs to resolve issues	Reduction in costs to optimize policies

How to get started with SD-Access

- Review the business and technical decision maker presentations
- Read the SD-Access Technical Solution white paper
- Ask your sales representative for a product demo

CISILION