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 is the industry's first intent-based networking solution for the Enterprise built on the principles of Cisco's Digital Network Architecture (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

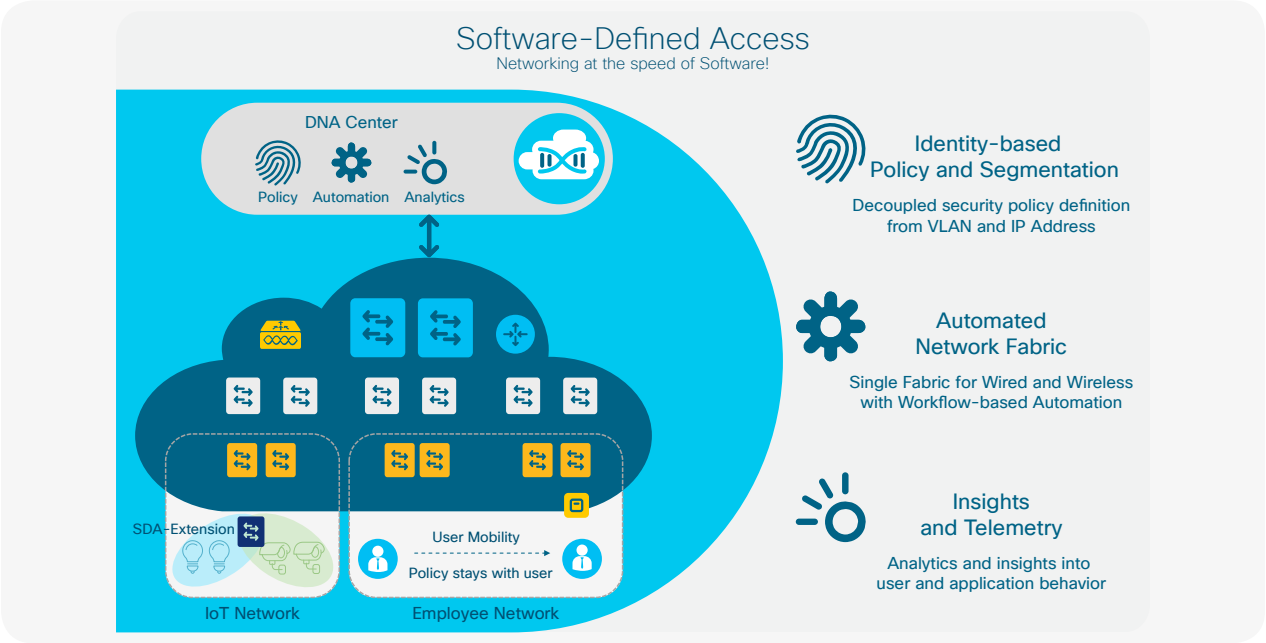
SD-Access solution overview

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



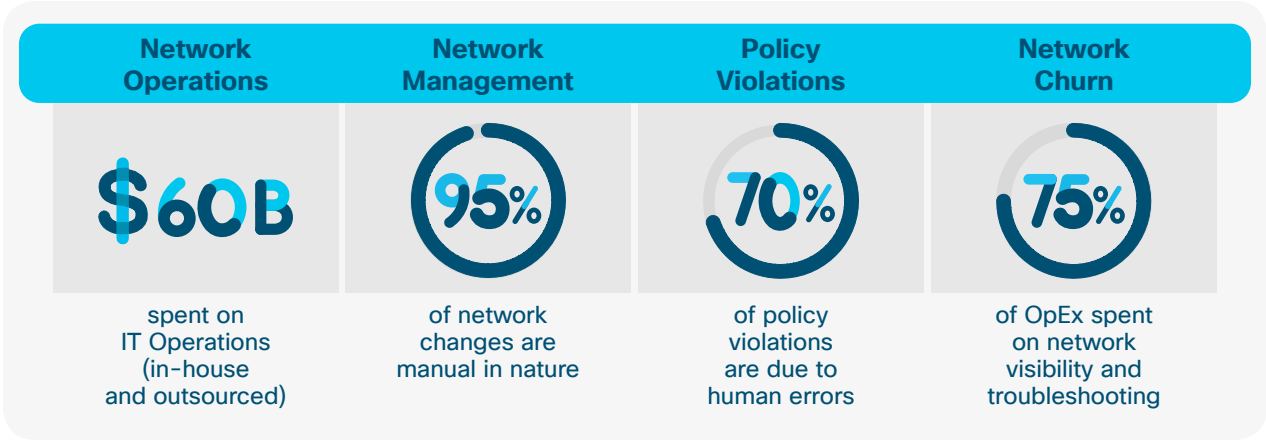
Why SD-Access?

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 will be 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, it is more complex to configure user credentials and maintain a consistent policy across the network. 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, it also becomes difficult to locate users and troubleshoot issues. The bottom line is that the networks of today do not address today's network needs.

Network fabric: With a controller element in place, it's sensible to 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, improved 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, Extranet, 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, using the NETCONF and YANG models; (3) granular visibility, using telemetry capabilities such as NetFlow; and (4) seamless software upgrades with live software patching.



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

Key features

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

Table 1. SD-Access 1.x (update 1.2.5) 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 Configs** (Update 1.1.3) • **ISR 4221 as a fabric border node** (Update 1.1.3) • **Enhancements in Underlay LAN Automation** (Update 1.1.3) • **Fabric Pre-Provisioning and Post-Provisioning Validations** (Update 1.1.3) • **SD-Access for Distributed Campus** (New in update 1.2.5) • **SD-Extension for IoT** (In product-beta-New in update 1.2.0) • **Cisco Catalyst 9300 Stack as Border node and Control Plane** (New in update 1.2.5) • **Connectivity between hosts in the fabric and an external Layer 2 domain** (New in update 1.2.5) • **Fabric-in-a-box wherein a device can be the edge, border and control nodes simultaneously** (New in update 1.2.5) • **Support for Broadcast, Link-local multicast traffic in the underlay** (New in update 1.2.5) • **Ability to assign a fabric edge switchport as a trunk to facilitate server connectivity** (New in update 1.2.5) • **Support for an internal border for DC connectivity** (New in update 1.2.4)
Fabric control plane	• Demand-based overlays with LISP-based control plane • Control plane co-located with fabric border or standalone • Resiliency-Support for multiple LISP control plane nodes • Support for six control plane nodes (New in update 1.2.5)

Feature	Description
Fabric Assurance	▪ KPIs, 360 views for Client, AP, WLC, and Switch – Underlay and Overlay Correlation – Device Health: Fabric Border and Edge; CPU, Memory, Temperature, Line cards, Modules, Stacking, PoE power, TCAM – Data plane 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 and DNS, Client authentication and authorization – Traffic Visualization and Network Service Assurance with LiveNX from LiveAction
Security	▪ Host Onboarding Enhancement-IBNS 2.0 (New in update 1.2)
Segmentation	▪ Network segmentation using Virtual Networks (VNs) and context-based groups ▪ 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 ▪ Identity (group) federation via pxGrid ▪ 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 domain ▪ 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 Following features are new in update 1.2: ▪ 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
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 full list of management features in DNA Center 1.2 here
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 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.

Note:

- Wave 1 access points won't support the following functions when deployed for SD-Access: IPv6, Application Visibility and Control (AVC), NetFlow.
- A device can act as fabric border and fabric control plane at the same time.

SDA Scale information

Table 2. SD-Access 1.2.5 overall scale

Fabric constructs	Maximum supported on single DNA Center cluster
No of fabric domains per DNA Center cluster	10
No of Fabric Sites across the Fabric Domains*	200
APs (Counted as Endpoints) per DNA Center cluster*	32K
Total Endpoints (including APs) per DNA Center cluster*	53K
Fabric Nodes (Edge, Border, WLC) per DNA Center cluster*	500**
Non-Fabric Nodes (Intermediate Routers and Switches) per DNA Center cluster*	1000
Control plane nodes per fabric site	6
Default border nodes per fabric site	4
IP Pools*	500
Groups (SGTs) per DNA Center Cluster*	4K
Number of access control policies per DNA Center cluster*	1K
Number of traffic copy policies per DNA Center cluster*	10
Number of contracts per DNA Center cluster*	500

* Above scale is split across all the configurable fabric domains (10) or can be in one fabric domain.

** A Stack of switches is considered as one Fabric Node

DNA Center is supported in a single node cluster or a three-node cluster. The three-node cluster provides high availability in the event of failed node.

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 total cost of ownership (Table 2).

Table 3. 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 wired and 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

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

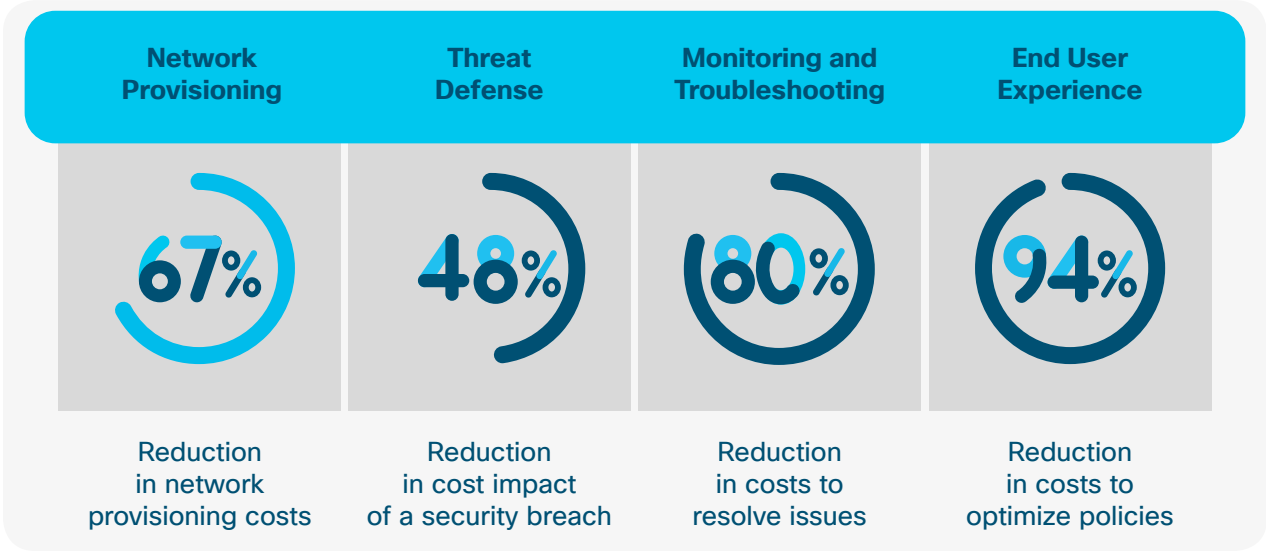
Cisco Capital

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.



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

C22-739012-10 10/18