Cisco Software-Defined Access

Introducing an entirely new era in networking.

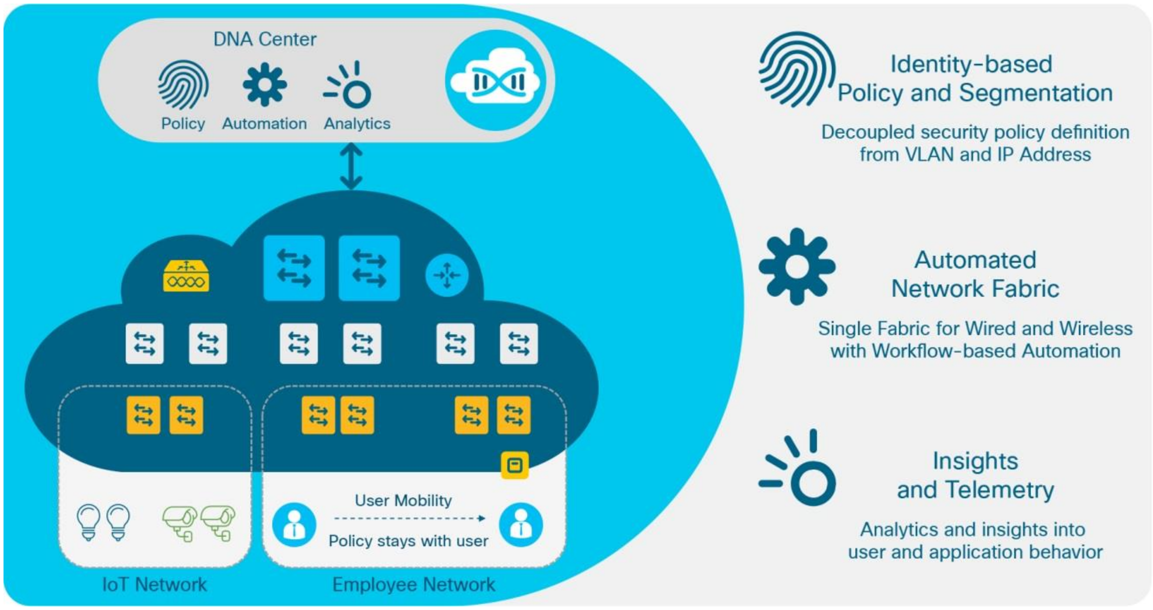
What if you could give time back to IT? Provide network access in minutes for any user or device to any application – without compromise?

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

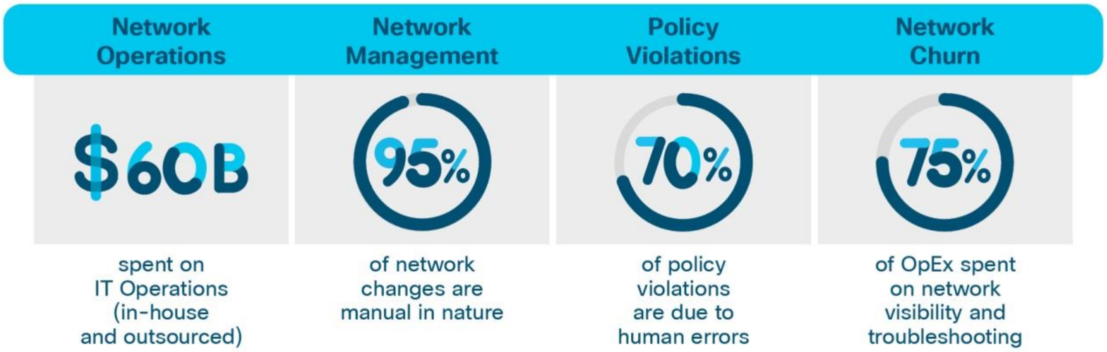
Figure 1. SD-Access Overview


DNA Center
Policy
Automation
Analytics
User Mobility
Policy stays with user
IoT Network
Employee Network
Identity-based Policy and Segmentation
Decoupled security policy definition from VLAN and IP Address
Automated Network Fabric
Single Fabric for Wired and Wireless with Workflow-based Automation
Insights and Telemetry
Analytics and insights into user and application behavior

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.



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.

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.

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.

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 the YANG operational model; and (4) seamless software upgrades with live software patching.

Solution Components

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

- Cisco DNA Center
- Cisco Identity Services Engine (ISE)
- Network platforms: See Table 3

Key Features

See Table 1 for a list of the key features of SD-Access 1.1

Table 1. SD-Access 1.1 Key Features

Feature	Description
Fabric infrastructure	• Virtual network overlays with virtual extensible LAN (VXLAN) • Default Anycast Layer 3 gateway (L3VNI) • Multicast support with Head-End Replication • Automated underlay and custom underlay options • Load balancing using Equal-Cost Multipath Routing (ECMP) in underlay • External connectivity handoff using Virtual Routing and Forwarding Lite (VRF-Lite), and Border Gateway Protocol Ethernet VPN (BGP-EVPN) (New in 1.1) • External connectivity handoff using Virtual Routing and Forwarding Lite (VRF-Lite), Multiprotocol Label Switching (MPLS), Dynamic Multipoint VPN (DMVPN), and Border Gateway Protocol Ethernet VPN (BGP-EVPN) (Manual) • Resiliency – Support for multiple Fabric Border Nodes
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
Fabric Assurance (New in 1.1)	• KPIs, 360 views for Client, AP, WLC, and Switch (In-Product Beta) ◦ Underlay & Overlay Correlation ◦ Device Health: Fabric Border and Edge; CPU, Memory, Temparature, 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
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
Fabric Wireless	• Enterprise wireless support • VXLAN support at access point • Distributed data plane for higher wireless performance • Seamless roaming within the fabric domain

Feature	Description
	• Wireless Guest with ISE (CWA) (New in 1.1) • Wireless Guest Support on Separate Guest Border/Control Plane and Wireless Guest Support as separate VN on Enterprise Border/Control Plane (New in 1.1) • Same SSID for Traditional and Fabric on same WLC (Mixed Mode) (New in 1.1) • WLC SSO (New 1.1) • Wireless Multicast (New 1.1)
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	• Single pane of management with Cisco DNA Center • Automatic fabric discovery • Consistent segmentation and policy for wired and wireless users and devices • Consistent provisioning for wired and wireless infrastructure • Pre-Check and Post-Check Workflow Validations (New in 1.1) • Role-Based Access Control (RBAC) • Authenticated access based on certificate authentication and local authentication • Northbound APIs – open Cisco IOS® XE device APIs and DNAC REST APIs • ISE PAN HA support (includes PxGrid, M&T) (New in 1.1) • Distributed ISE PSN support (2 per Site) (New in 1.1) • Same ISE Instance for Fabric and Traditional (Brownfield) Deployments (New in 1.1) • ACS/ISE for Tacacs+ Authentication of Network Devices (New in 1.1) • HA Support for DNAC (New in 1.1) • Policy protected CLI configuration (New in 1.1) • Software Image and Patch Management (New in 1.1) • License Management (New in 1.1) • Backup and Restore (New in 1.1) • Task Scheduler (New in 1.1)
Technology partners	• IPAM – Infoblox • Integrated threat defense – Cisco Stealthwatch® • Firewalls – Cisco ASA, Cisco Firepower® Threat Defense • Policy orchestrators – Tufin, Algosec

Table 2. SD-Access 1.1 Hardware and Software Compatibility Matrix

Management	DNA Center	DNA 1.1 (Appliance only)
Identity	Identity Services Engine	ISE 2.3 patch 1
Fabric edge	Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches (Sup1) Cisco Catalyst 3850 Series and 3650 Series Switches Cisco Catalyst 4500E Series Switches (Sup8E, Sup9E)	IOS-XE 16.6.2s IOS-XE 16.6.2s IOS-XE 16.6.2s IOS 3.10.0cE
Fabric border and control plane	Cisco Catalyst 9500 Series Switches Cisco Catalyst 3850 Series Fiber Module Cisco Catalyst 6807-XL Switch (Sup6T, Sup2T) Cisco Catalyst 6500 Series Switches Cisco Catalyst 6880-X Switch Cisco Catalyst 6840-X Switch Cisco Nexus® 7700 Switch (Sup 2E, M3 line cards only) Cisco 4000 Series Integrated Services Routers Cisco ASR 1000 Series Aggregation Services Routers Cisco Cloud Services Router 1000v (control plane only)	IOS-XE 16.6.2s IOS-XE 16.6.2s IOS 15.4(1)SY3 IOS 15.4(1)SY3 IOS 15.4(1)SY3 IOS 15.4(1)SY3 NX-OS 8.2(1) IOS-XE 16.6.2 IOS-XE 16.6.2 IOS-XE 16.6.2
SD-Access wireless	802.11 Wave 2 access points: Cisco Aironet® 1800, 2800, and 3800 Series 802.11 Wave 1 access points: Cisco Aironet® 1700, 2700, and 3700 Series Cisco 3504, 5520 and 8540 Series Wireless Controllers	AireOS 8.5.110.0 MR1 AireOS 8.5.110.0 MR1 AireOS 8.5.110.0 MR1

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 cannot act as fabric edge and fabric border at the same time.
- A device can act as fabric border and fabric control plane at the same time.

SD-Access Use Cases

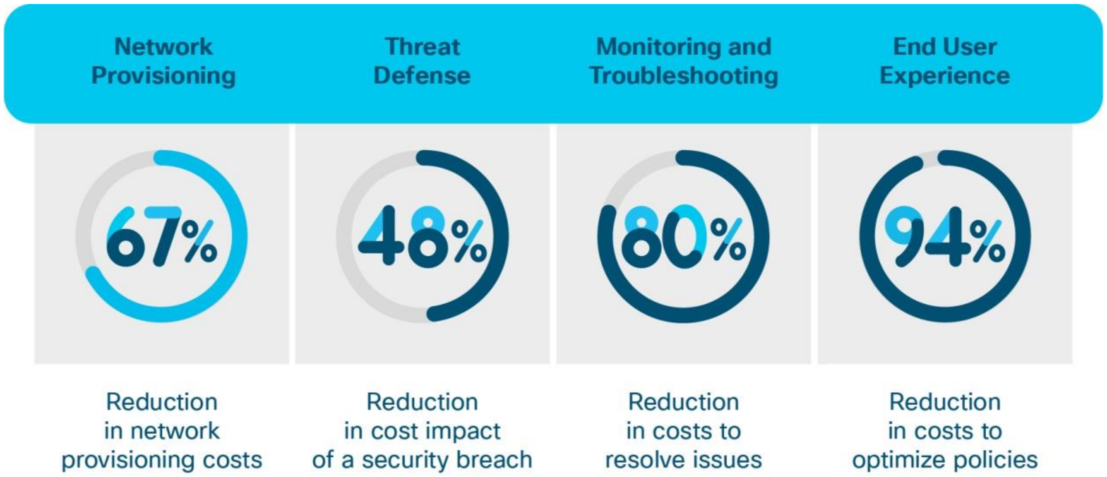
Building on the foundation of industry-leading capabilities, SD-Access can now deliver key business-driven use cases that truly realize the promise of a digital enterprise while reducing total cost of ownership (Table 3).

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 between wired and wireless • Distributed data plane for wireless access • Simplified guest provisioning for wired and 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
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

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.



Ordering Information

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

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital® can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

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

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C22-739012-03 12/17