Cisco Software-Defined Access

Introducing an entirely new era in networking. The Network. Intuitive.

What if you could give time back to IT? Provide network access in minutes for any user or device to any application – without compromise? We give you the industry's first policy-based automation from network edge to cloud. Your foundation for your digital network, Cisco® Software-Defined Access (SD-Access). Built on the principles of the Cisco Digital Network Architecture (Cisco DNA™), SD-Access provides end-to-end segmentation to keep user, device and application traffic separate without a redesign of the network. It automates user access policy so organizations can make sure the right policies are set for any user or device with any application across the network. This is all done with a single network fabric, to enable a consistent user experience anywhere without compromising on security, meaning common user policy for LAN, WAN and cloud.

Maintaining policy is getting more difficult and the configuration process is more complex. With more users and endpoints, the network is difficult to segment. IT often ends up with separate user policies for wired and wireless networks and is unable to find users when troubleshooting. More users, more policies, more complexity. You need a network built on experience that can turn context into intelligence. A network that can respond faster, in a more human way. The Network. Intuitive.

Benefits

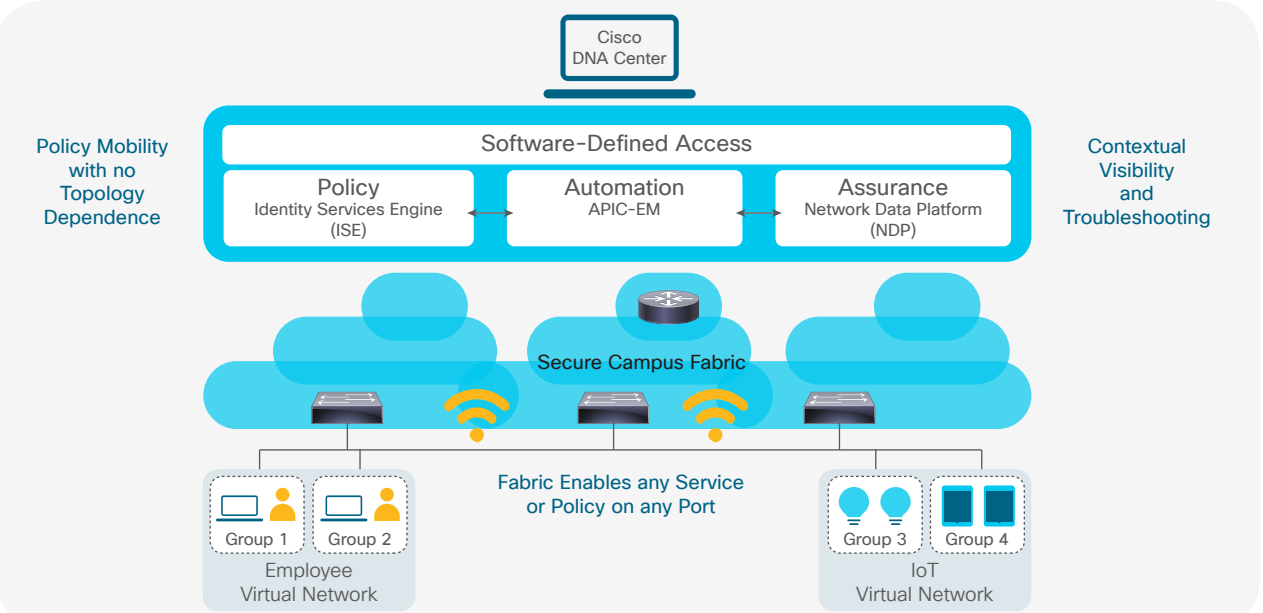
- **Use policy-based automated network provisioning** from edge to cloud
- **Quickly enable services** by using turnkey automation and open APIs across the services ecosystem
- **Gain visibility** into the entire network, with wired, wireless and WAN managed as a single entity
- **Lower operational expenses,** building on existing infrastructure to become more efficient

The Cisco advantage

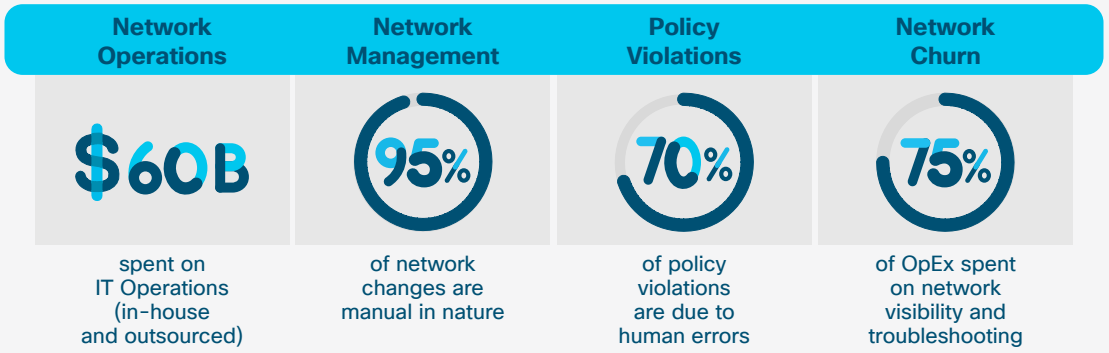
Why the need for SD-Access? There are many challenges today in managing the network to drive business outcomes. These limitations are due to manual configuration and fragmented tool offerings. SD-Access provides:

- A transformational management solution that reduces operational expenses and enhances business agility
- 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 and the Digital Network Architecture



Challenges



The solution – SD-Access

Cisco is constantly striving to solve key challenges faced by corporate IT departments by developing important technologies to drive transformation.

To understand the fundamental benefits of SD-Access, it's important to look at both the foundational and functional aspects of this solution.

Table 1. IT transformational goals (summarizes some of the key priorities for IT.)

IT Priorities	Network Infrastructure Requirements
Operational effectiveness: ▪ Network automation ▪ Network assurance ▪ Network convergence ▪ Alignment with "cloud first"	▪ Consistent, standards-based APIs ▪ Policy automation (installation and provisioning) ▪ Network virtualization and segmentation ▪ Resiliency, scale, high availability ▪ Secure cloud connectivity
Improved workforce experience: ▪ Collaboration ▪ Bring Your Own Device (BYOD) and mobility	▪ Intelligent traffic engineering (application based) ▪ Application visibility and control, dynamic Quality of Service (QoS) ▪ Network access control and Mobile Device Management (MDM) ▪ Network virtualization and segmentation
Security and compliance	▪ Threat visibility and authenticated network access ▪ Role-based internal network segmentation ▪ Dynamic service insertion

These challenges are deeply rooted within network deployment and operations:

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.

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.

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.

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

Foundational concepts

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 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. In SD-Access, a fabric is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric in place enables several capabilities, such as the creation of virtual networks and user and device groups and SD-WAN integration and advanced reporting. 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.

Functional features

Network design and deployment: The first step in building a network is to install devices and build a basic infrastructure to support the business. Cisco DNA Center provides a design center that allows the network architect or administrator to design the network and generate configuration commands for the relevant devices. This is possible by leveraging Cisco Validated Designs that have been fully tested and certified to meet customer deployment needs and scale.

Solution components

SD-Access is built on industry-leading software and hardware components.

The core components are:

- Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 2.0, including Cisco DNA Center
- Identity Services Engine (ISE)
- Network Data Platform
- Network devices: See Table 2

Network segmentation: Many medium-sized to large businesses want to consolidate multiple networks into one management plane while having the ability to segment the network into either lines of business or functional blocks.

Flexible authentication options: Devices and users require secure connections to the corporate network using various authentication schemes. SD-Access provides flexibility, with options such as 802.1X, Active Directory and static authentication schemes.

Group-based policy: Enabling policy on a traditional network can be complex, so it is critical be able to collect users or devices into groups regardless of IP address or VLAN membership. Once these are in place, policies can be created describing how these groups interact with each other from the Cisco DNA Center policy screens. SD-Access uses the industry-leading and proven Cisco TrustSec® technology to deliver this capability across the enterprise.

Network assurance: Network downtime and user connectivity issues can dramatically affect business revenue and productivity. Businesses want the ability to predict issues and take proactive measures as well as resolve issues expeditiously whenever they occur. Cisco DNA Center assurance capabilities collect data from many sources in the network, such as syslog and NetFlow, to provide contextual insights into users and network activities.

Table 2. Matrix of supported device platforms, including network roles

	Access	Border
Fixed	Cisco Catalyst® 9300 Series Cisco Catalyst 3850 Series Catalyst 3650 Series 802.11 Wave 2 access points: Cisco Aironet® 1800, 2800 and 3800 Series Cisco 5520 and 8540 Wireless Controllers	Cisco Catalyst 9500 Series Cisco Catalyst 3850 Series 10G models Cisco Catalyst 4500-X Series Cisco 4000 Series Integrated Services Routers Cisco ASR 1000 Series Aggregation Services Routers
Modular	Cisco Catalyst 9400 Series (Sup1) Cisco Catalyst 4500E Series (Sup8E, Sup9E)	Cisco Catalyst 6807-XL (Sup6T, Sup2T) Cisco Catalyst 6500 Series Cisco Catalyst 6880-X Cisco Catalyst 6840-X Cisco Nexus® 7700 (Sup 2E, M3 Line Cards only)

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 Virtual Routing and Forwarding (VRF) configuration (lines of business, departments, etc.)	▪ Reduce time to provision network segmentation and user groups ▪ Provide a foundation to enforce network security policies
User mobility	▪ Single point of definition for wired and wireless users ▪ Seamless roaming between wired and wireless	▪ Management of wired and wireless networks and users from a single interface (Cisco DNA Center) ▪ Offload wireless data path to network switches (reduce load on controller)
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	▪ Significant reduction in troubleshooting time ▪ Rich context and analytics for decision making

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
- Get a quick TCO analysis at http://cisco.com/go/sd-access/tco

Use Case	Details	Benefits
Cloud integration	▪ Policy management for user-to-application access ▪ Full integration with Cisco cloud solutions	▪ Administrator can define user-to-application access policy from a single interface ▪ End-to-end policy management for the enterprise
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 ▪ Enterprise-wide policy provisioning and enforcement

C22-739012-01 07/17