RED RIVER VIEWPOINT

MARCH 2019

CISCO SOFTWARE DEFINED ACCESS (SDA)

By Sonny Sachdeva

Red River

TECHNOLOGY DECISIONS AREN'T BLACK AND WHITE. **THINK RED.**

IN THIS PAPER

1. INTENT AND AUDIENCE

This document presents the strategic benefits of Cisco Software Defined Access (SDA) to the technical decision makers of organizations.

1.1 INTRODUCTION

What would it mean to your organization if you could improve its revenue and profitability while also making it more agile and competitive? Cisco's Software Defined Access (SDA) is a virtual, wireless and wired campus network that enables organizations to achieve these goals by utilizing automation, analytics, programmability, and integrated security.

Technology is a strategic asset allowing businesses to differentiate themselves and get close to their customers, leading to improved top and bottom lines. According to the MIT Center for Digital Business, 90 percent of CEOs believe digital will have significant impact on their business and per Gartner, 56 percent of the CEOs say that digitization of their business improved their net profit. Harvard Business Review also found that companies who master digital transformation generate 9 percent more revenue and 26 percent more profits than their industry peers[i].

1.2 WHAT DOES IT MEAN TO BE DIGITAL?

In the context of Software Defined Networking, digital means to be automated via programmable hardware, to have integrated security within the network and to utilize deep, actionable analytics.

2. CURRENT STATE

Organizations need their applications to be highly available and responsive at all times. The network serves as the cohesive fabric connecting the servers and storage infrastructure to the clients. It needs to be consistently available and be flexible for maintenance windows.

According to a study performed by McKinsey in 2016, IT teams spend 43 percent of their time troubleshooting issues and the majority of that time is spent on gathering data rather than analyzing the root cause[ii]. In addition, troubleshooting is difficult as the issues are hard to replicate and it can take hours to either resolve the issue or prove that the network is not the root cause. IT spends 3x more on network operations vs. network deployment[iii] and it can take an average of six months to detect a security breach[iv]. These problems will only be exacerbated as 63 million new devices are projected to come online every second by 2020[v].

The past few years have seen great leaps in technology such as virtualization and public cloud, which are allowing greater efficiencies and application availability at a reduced cost. Server virtualization not only made hardware utilization more efficient, it also made business continuity and disaster recovery more practical. Public cloud has lowered the barrier to entry for startups and in doing so, increased competition.

Digital businesses require a programmable network that is flexible and responsive.

Current networks are complex to deploy, manage and segment, and difficult to troubleshoot. Where Server Virtualization has led to automation and orchestration which allows us to create and manage virtual machines at scale, the networking world is still manually configuring each device which is time consuming and error prone.

Network management tools have to be purchased separately and provide basic alerts which may be ignored as they become overwhelming in a large environment. Troubleshooting times are prolonged due to incomplete inventory discovery, the need to log into each device individually, and translating a user's identity into MAC and IP addresses.

Network security via segmentation is based on manipulating network constructs such as VLANs, Subnets, IP addresses, and TCP/UDP ports. Securing a new group of users or devices entails creating new VLANs, extending them to the access, distribution and core switches, and creating new Access-lists and/or VRFs to segment them from the existing environment.

IoT will compound these problems as more devices are being on-boarded without adequate processing power to protect themselves from threats.

3. WHY SHOULD BUSINESSES ADOPT SDA?

Digital businesses require a programmable network that is flexible and responsive. Cisco Software Defined Access (SDA) improves upon the current architecture by providing a secure and intent aware network which simplifies deployment and operations. **The business intent** is defined in software, and then that policy is centrally deployed into the programmable hardware infrastructure.

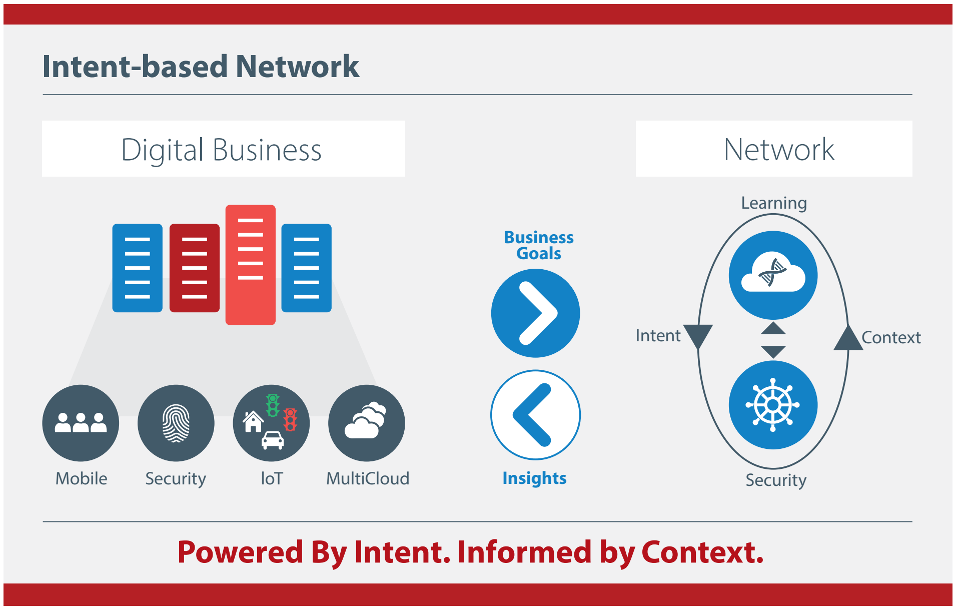


Figure 1: SDA Framework – Cisco Presentation

DNAC also simplifies and automates security via integration with ISE, allowing network wide deployment of the security policies onto the network infrastructure.

The SDA framework consists of the DNA Center (DNAC), Identity Services Engine (ISE), and the supporting wired and wireless infrastructure.

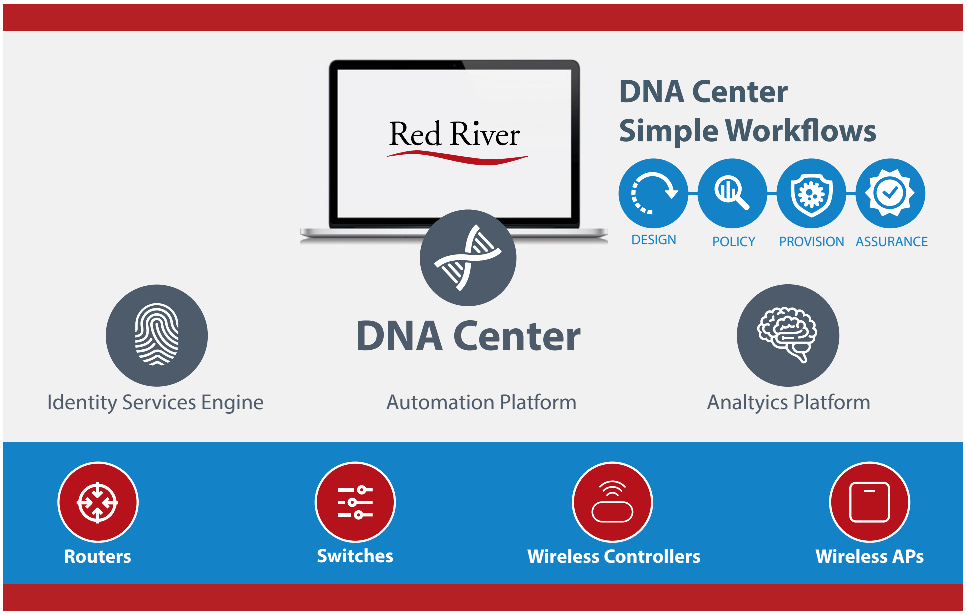


Figure 2: DNA Center – Cisco Presentation

The DNAC consists of two components – the ***Automation Platform*** and the ***Analytics Platform.***

The DNAC is where the intent is captured and translated into configurations. For example, the intent of deploying SD-WAN between multiple sites is translated into configurations of Quality of Service (QoS), Performance Routing (PfR), and IPSec/Generic Routing Encapsulation (GRE) tunnels. These configurations are then deployed on the target devices to realize the original intent.

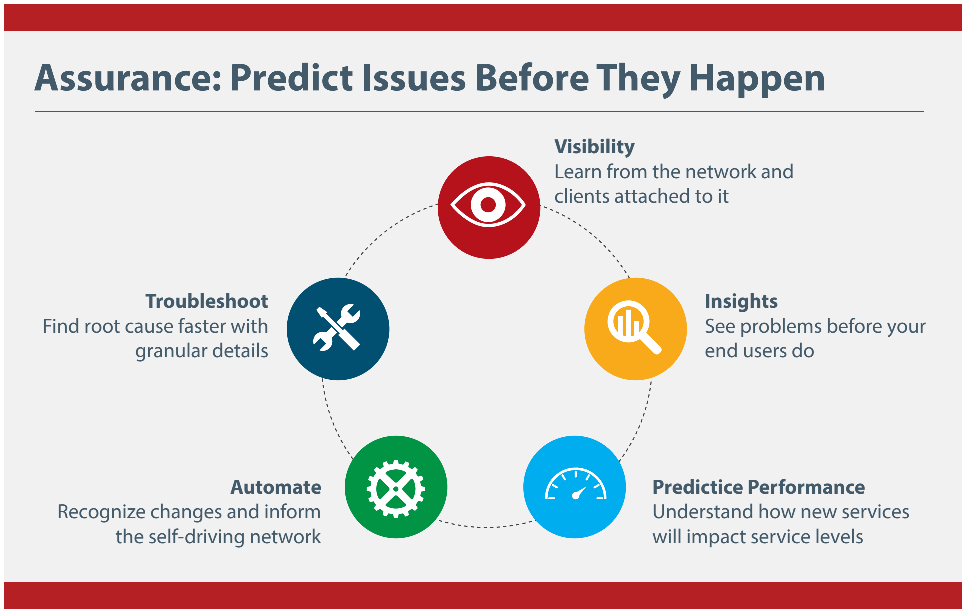
3.1 AUTOMATION PLATFORM

Cisco SDA reduces human error and deployment time via ***Automation*** which allows standardization of device configurations and policies to be implemented holistically on the entire network rather than on a per device basis.

Cisco SDA automatically discovers the switching infrastructure and creates an Underlay and an Overlay network. The Underlay provides a stable and redundant foundation that is well defined and invisible to endpoints. The Overlay provides a dynamic network that is constantly learning about new apps, devices, and users and is constantly adapting to their needs. The policy is decoupled and implemented in the Overlay independent of the Underlay, thereby drastically reducing the downtime related to device misconfigurations and human errors resulting from moves, adds and changes.

DNAC also simplifies and automates security via integration with ISE, allowing network wide deployment of the security policies onto the network infrastructure.

3.2 NETWORK ANALYTICS PLATFORM



Assurance: Predict Issues Before They Happen

Visibility
Learn from the network and clients attached to it

Insights
See problems before your end users do

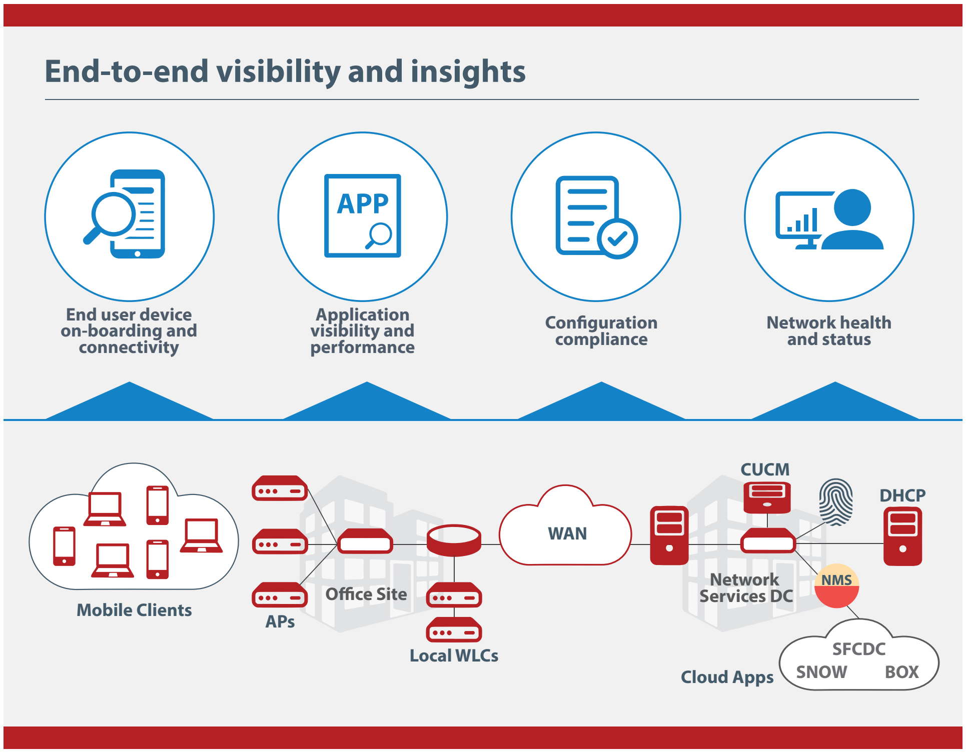
Predictice Performance
Understand how new services will impact service levels

Automate
Recognize changes and inform the self-driving network

Troubleshoot
Find root cause faster with granular details

Figure 3: Assurance through Predictive Analysis – Cisco Presentation

***Cisco Assurance* transforms data into business value** by reducing the time needed for data gathering and analysis. Device data such as Simple Network Management Protocol (SNMP), Netflow and logs can be gathered and correlated using machine learning algorithms and can be transformed into **actionable intelligence.** Issues can be proactively identified and remediated before the users experience an outage.



End-to-end visibility and insights

End user device on-boarding and connectivity

Application visibility and performance

Configuration compliance

Network health and status

Figure 4: End-to-End Visibility – Cisco Presentation

Cisco SDA provides end-to-end visibility and provides context such as, "20 clients are having trouble onboarding at an AP" rather than a series of alerts.

Troubleshooting the network is particularly complex due to its size and scale. Cisco SDA provides end-to-end visibility and provides context such as, "20 clients are having trouble onboarding at an AP" rather than a series of alerts.

Assurance is fundamentally different than the current Network Management Platforms which gather data based on SNMP polls and traps, and utilize scripts and templates to assist in device configuration. It dramatically lowers the time needed for troubleshooting by providing new tools such as Path Trace which provide 360-degree contextual insights by presenting all L3 and L2 devices in the path. ***Assurance* can then provide deeper, configuration level insight** into each device to find the root cause such as a misconfigured Access-list.

Ticket escalations can be prevented by guided troubleshooting that can lead the Network Operations engineer step-by-step through the process by simply clicking "run" without ever having to leave the graphical user interface (GUI). There is no longer a need to log into individual devices via command line interface (CLI). A DVR-like timeline feature eliminates the "failure to replicate issue" problem and can be used to revisit the moment when the issue occurred, identify the cause, and prevent it from reoccurring. Small sensors can proactively test the network and provide current state data.

Using machine learning algorithms, trends can be proactively identified before users experience an issue. The Network team can also increase its accuracy by providing feedback on its predictions. In the future this can enable **self-remediation** where previously learned steps can be automatically executed to resolve an issue.

3.3 SECURITY PLATFORM

***Security* is designed from inception** in the SDA framework through the integration of Identity Services Engine (ISE). Segmenting traffic by departments or by groups no longer needs to involve tedious and time-consuming work of configuring VLANs, IP addresses, and ports; instead each user's data can be tagged and controlled directly.

Traffic can be **macro-segmented** between groups or **micro-segmented** within a user group, removing the need for access-lists which continue to litter the firewall - a practice which has caused security holes and exposed organizations to hackers. The threat landscape is ever evolving and manual interventions are insufficient. Python and Rest application programming interface (API) integration allows machine-to-machine communication and coordination which dramatically decreases the reaction time.

As more traffic becomes encrypted by secure sockets layer (SSL), the malware is also becoming encrypted. SDA allows us to check for malware in SSL encrypted traffic without the need for decryption.

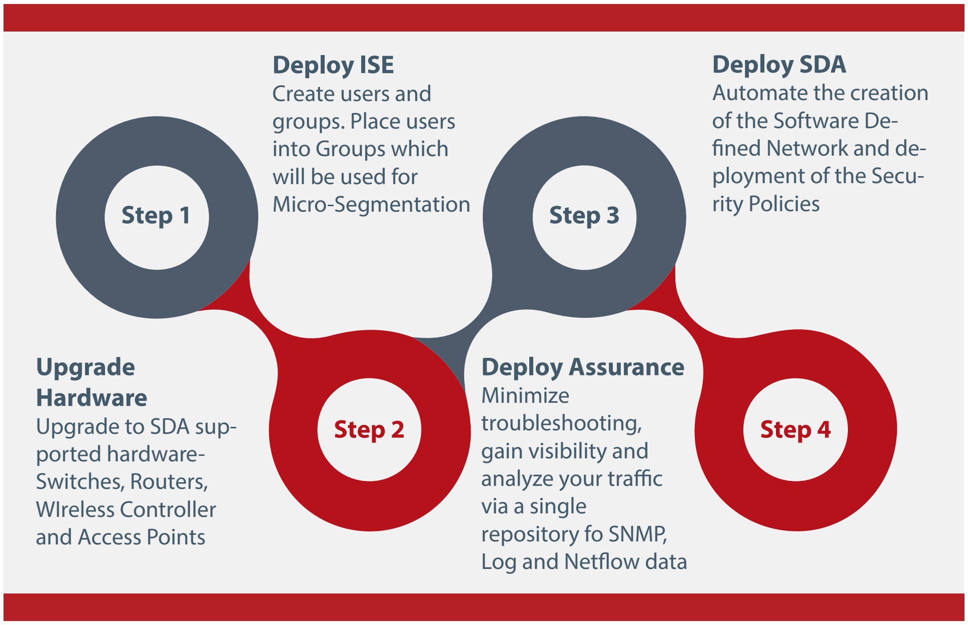
Wired and wireless traffic policies are managed in a consistent and unified fashion utilizing User Identity and group membership to provide micro-segmentation of traffic. **Traffic encryption** provides an additional layer of security from snooping attacks if the network is infiltrated. Users are authenticated and their actions are authorized by ISE. Security policy can now be defined based on user/device profiles consisting of contextual attributes such as who, what, where, and when and not solely IP or MAC addresses.

3.4 PROGRAMMABILITY

Python and REST APIs enable **machine-to-machine** communication allowing operations at scale without human intervention. They also provide users direct access to **customize SDA** and create their own custom interface or functions.

Cisco SDA is a paradigm shift in networking for the 21st century, uniting wired, wireless, security, insight, and intelligence into one platform that will dramatically improve the user experience.

Cisco is also partnering with vendors such as ServiceNow to allow API connectivity between both systems where Assurance could recognize an issue and open a service ticket for human approval. Assurance can then resolve the issue automatically, thanks to Guided Machine learning and then send the message to the ticketing platform to close the ticket.



Upgrade Hardware
Upgrade to SDA supported hardware- Switches, Routers, WIreless Controller and Access Points

Deploy ISE
Create users and groups. Place users into Groups which will be used for Micro-Segmentation

Deploy Assurance
Minimize troubleshooting, gain visibility and analyze your traffic via a single repository fo SNMP, Log and Netflow data

Deploy SDA
Automate the creation of the Software Defined Network and deployment of the Security Policies

Figure 5

3.5 JOURNEY TO SDA

Red River recommends the journey mentioned above for a Production environment to ensure a smooth and successful transition. Some of the steps such as network upgrade and deployment of ISE could be performed in parallel or reversed depending on the condition of the environment and the expertise of the IT team.

1. The existing wired and wireless hardware should be upgraded to the SDA supported hardware. The complete and updated list of SDA supported devices can be found here. We recommend that an SDA lab bundle be purchased along with the network upgrade to acclimate the IT team to the new user interface and functionality. SDA is revolutionary and it will require time to get acclimated to the new processes.

2. ISE could be deployed for basic TACACS+ functionality to secure logins to the network infrastructure and for securing wireless employees and guest access. More specific users and groups can be planned in anticipation of the full SDA rollout in the future.

3. Assurance could be phased in over time in parallel with the existing network management system until it is no longer needed. For example, a building from the campus network could be migrated to Assurance and Cisco Prime could continue to run in parallel due to its robust reporting capability.

4. Finally, SDA can be used to create a fabric and easily deploy security policies based on contextual user attributes once the wired and wireless hardware is upgraded and the user groups are configured in ISE.

Finally, programmability provides flexibility and allows open communication and customization with users and partners.

4. CONCLUSION

The days of a fragmented network which was difficult to deploy, manage, and troubleshoot are numbered. Cisco SDA is a paradigm shift in networking for the 21st century, uniting wired, wireless, security, insight, and intelligence into one platform that will dramatically improve the user experience.

SDA fundamenally transforms the network by driving policy via automation and orchestration; discovering and provisioning the network infrastructure in an intuitive manner leading to simpler deployments, decreasing change windows and human error.

Assurance reduces time needed for troubleshooting and simplifies management leading to a better user experience. It simplifies troubleshooting by displaying 360-degree contextual information which can be acted upon to resolve the root cause by providing a DVR-like functionality to aid in identifying and tracing historical data to identify and resolve issues. Issues can be identified proactively using machine-learning before they become problems. Ticket escalations can be reduced due to guided troubleshooting.

ISE secures the network by delivering micro-segmentation of traffic based on user attributes and eases troubleshooting by eliminating legacy network constructs as security tools.

Programmability allows Cisco's eco-system partners, customers and developer community to build custom solutions and tools using open APIs. Cisco DevNet is very healthy and thriving community of developers that is open to all partners, and customers.

Cisco SDA provides a centralized, intent-based networking platform that addresses the inadequacies of traditional way of building and deploying networks. Network design, deployment, management and security are addressed holistically thereby allowing organizations to scale and execute at the pace of business.

5. THE RED RIVER DIFFERENCE

Red River has more than 20 years of experience serving customers in the commercial, civilian, defense, intelligence, healthcare, and SLED markets. We have built a tremendous reputation among them for our superior expertise and personal touch. It is our mission to reimagine the possibilities of technology to create a positive impact on the people and organizations we serve. We understand your mission and offer the capabilities and technology required to solve your critical data center, security, analytics, cloud, network, collaboration and mobility challenges.

5.1 RED RIVER OFFERINGS

Red River leads customers on their journey to SDA. We offer planning and design of the multi-step journey including:

Infrastructure discovery and assessment

- ROI analysis
- Detailed design Services
- Quick Start – Lab Bundle
- Consulting Services
- Managed Services

5.2 ABOUT THE AUTHOR

Sonny Sachdeva has been helping organizations with their technological needs for over twenty years. His experience includes designing, implementing and managing networks, datacenters and hybrid clouds across all verticals. During this time, he has also acquired various distinguished certifications such as the Cisco CCIE in Datacenter and Routing & Switching, VMware VCP and Amazon AWS Solutions Architect Professional. He is passionate about helping people, technology, traveling and learning something new each day. Sonny resides with his wife and two kids in sunny Fort Lauderdale and enjoys taking walks, biking and going to the beach with his family.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 20 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions.

Learn more at **redriver.com.**

[i] https://hbr.org/product/leading-digital-turning-technology-into-business-transformation/17039E-KND-ENG
[ii] McKinsey Study of Network Operations for Cisco - 2016
[iii] McKinsey Study of Network Operations for Cisco - 2016
[iv] Ponemon Research Institute Study on Malware Detection, March 2016
[v] Gartner Report – Gartner's 2017 Strategic Roadmap for Networking

CONTACT US

Contact Red River today to speak with one of our Solutions Architects and begin your journey.

✉ info@redriver.com

☎ 800.769.3060

RED RIVER
Corporate Headquarters
21 Water St., Suite 500
Claremont, NH 03743
800.769.3060 toll free
603.448.8880 phone
603.448.8844 fax

www.redriver.com

Red River