Cisco Software-Defined Access

Cisco Secure Enterprise

Jason Gooley, CCIE® x2 (RS & SP) No. 38759
Roddie Hasan, CCIE® RS No. 7472
Srilatha Vemula, CCIE® SEC No. 33670

ciscopress.com

Cisco Software-Defined Access

Jason Gooley, CCIE No. 38759
Roddie Hasan, CCIE No. 7472
Srilatha Vemula, CCIE No. 33670

Cisco Press

Cisco Software-Defined Access

Jason Gooley

Roddie Hasan

Srilatha Vemula

Published by:
Cisco Press
Hoboken, NJ

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020938615

ISBN-13: 978-0-13-644838-9

ISBN-10: 0-13-644838-0

Warning and Disclaimer

This book is designed to provide information about Cisco Software-Defined Access (Cisco SD-Access). Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Arezou Gol

Director, ITP Product Management: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Marianne Bartow

Senior Project Editor: Tonya Simpson

Copy Editor: Bill McManus

Technical Editors: Dax Mickelson, Nicole Wajer

Editorial Assistant: Cindy Teeters

Book Designer: Chuti Pratsertsith

Composition: codeMantra

Indexer: Timothy Wright

Proofreader: Gill Editorial Services

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 **www.cisco.com/go/offices.**

About the Authors

Jason Gooley, CCIE No. 38759 (RS and SP), is a very enthusiastic and spontaneous person who has more than 25 years of experience in the industry. Currently, Jason works as a technical evangelist for the Worldwide Enterprise Networking sales team at Cisco Systems. Jason is very passionate about helping others in the industry succeed. In addition to being a Cisco Press author, Jason is a distinguished speaker at CiscoLive, contributes to the development of the Cisco CCIE and DevNet exams, provides training for Learning@Cisco, is an active CCIE mentor, is a committee member for the Cisco Continuing Education Program (CE), and is a program committee member of the Chicago Network Operators Group (CHI-NOG), www.chinog.org. Jason also hosts a show called MetalDevOps. Jason can be found at www.MetalDevOps.com, @MetalDevOps, and @Jason_Gooley on all social media platforms.

Roddie Hasan, CCIE No. 7472 (RS), is a technical solutions architect for Cisco Systems and has 29 years of networking experience. He has been with Cisco for more than 12 years and is a subject matter expert on enterprise networks. His role is supporting customers and account teams globally, with a focus on Cisco DNA Center and Cisco Software-Defined Access. He also specializes in technologies such as MPLS, Enterprise BGP, and SD-WAN. Prior to joining Cisco, Roddie worked in the U.S. federal government and service provider verticals. Roddie blogs at www.ccie.tv and can be found on Twitter at @eiddor.

Srilatha Vemula, CCIE No. 33670 (SEC), is a technical solutions architect for the Worldwide Enterprise Networking Sales team at Cisco Systems. There, she works with account teams and systems engineers to help Cisco customers adopt Cisco DNA Center, Cisco SD-Access, Cisco Identity Services Engine, and Cisco TrustSec. Srilatha has served in multiple roles at Cisco, including technical consulting engineer and security solutions architect. She led the design and implementation of security projects using Cisco flagship security products for key U.S. financial customers.

About the Technical Reviewers

Dax Mickelson has been working in network engineering for more than 20 years. Most of this time has been spent building training material and labs for Cisco. Dax has obtained many industry certifications over the years, including Cisco Certified Internetwork Expert Written (CCIE Written); Cisco Certified Network Associate (CCNA); Cisco IP Telephony Support Specialist (CIPT); Cisco Certified Network Professional (CCNP); Cisco Certified Academy Instructor (CCAI); Linux Certified Instructor (LCI); Linux Certified Administrator (LCA); Mitel 3300 ICP Installation and Maintenance Certified (this includes several periphery certifications like teleworker); NEC IPKII Basic, Advanced, and IP Certified; Oracle Certified Professional (OCP/DBO); Certified Novell Administrator (CNA); Cradle Point Network Associate and Professional (CPCNA and CPCNP).

Nicole Wajer graduated with a degree in computer science from the Amsterdam University of Applied Sciences and specializes in security, Cisco DNA, the Internet of Things (IoT), and IPv6. She has a global role for the security aspects of Cisco SDA-Access and SD-WAN on the Enterprise Networking team as a technical solutions architect (IBN security).

Nicole's career with Cisco started in routing and switching and network security, but fighting spam and malware turned out to be in her "Cisco DNA" since her first day on the Internet, so a move to content security was an obvious progression. Nicole then joined the Enterprise Networking team to continue her security passion and progress with Cisco DNA Center.

Dedications

Jason Gooley:

This book is dedicated to my wife, Jamie, and my children, Kaleigh and Jaxon. I love you all more than anything! I also want to dedicate this book to my father and brother for always having my back. In addition, this book is dedicated to all the people who have supported me over the years and all the candidates who are studying or trying to improve themselves through education.

Roddie Hasan:

To my mother, Sylvia: You taught me the phrase "to make a long story short." I dedicate this to you, whose story ended up being too short. I miss you, Mom.

Srilatha Vemula:

This book is dedicated to my parents, Adiseshu and Lakshmi, and my sisters for your love and support. Your sacrifices and lessons opened up doors to opportunities in my life that wouldn't have been possible without you. Throughout the years of my personal and professional life, I learned a lot from friends, co-workers, and mentors who have made me a better person. I would also like to dedicate this book to those who have had a positive influence in my life.

Acknowledgments

Jason:

Thank you to Brett and Marianne Bartow as well as everyone else involved at Cisco Press. Not only do you make sure the books are top notch, you make me a better author!

Thank you to my team, Worldwide Enterprise Networking Sales at Cisco, for always supporting me through all the awesome projects I am fortunate enough to be a part of. #TeamGSD

Thank you to all the people who follow me on my journey, whether through social media or in person. You are much appreciated!

Roddie:

Thank you to Brett, Marianne, and all the staff at Cisco Press for putting up with my nonsense as I struggled to transition from an in-person communication style to a writing one. I learned a lot during this process thanks to your expertise and guidance.

Thank you to Jason Gooley for setting up this project for us, for your patience with chapter delay after chapter delay, and for being an amazing co-author along with Srilatha Vemula.

Thank you to all the amazing and sharp people at Cisco that I have worked with for the past 12 years for helping me grow in this field and helping get me to a point where I was ready to write a book.

And finally, and most importantly: Thank you to my wife, Erin, and kids, Sousan and Brian, for supporting me throughout my career and understanding when I had to go do "nerd stuff."

Srilatha:

Thank you, Cisco Press, especially Brett and Marianne Bartow, for your help and guidance through my first book. Thank you to the technical editors, Nicole Wajer and Dax Mickelson, for reviewing our work and making the book better. Thank you to my friend, mentor, and a fellow author Vivek Santuka for your guidance throughout the years.

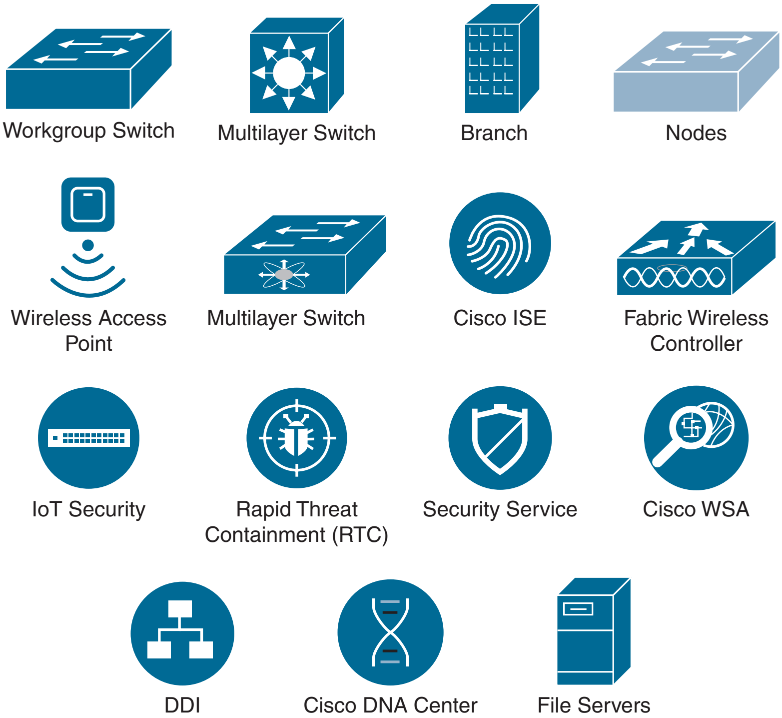
Thank you to my co-authors Jason Gooley and Roddie Hasan for the collaboration and making this fun.

Thank you to my team and Cisco for taking a chance on me. I am grateful for the opportunity to work for Cisco.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

This book was written to address the technical benefits and features of Cisco Software-Defined Access (Cisco SD-Access). This book is designed to deliver a use-case-based approach to implementing and adopting Cisco SD-Access in your organization. In addition, readers will learn when and where to leverage Cisco SD-Access instead of a typical three-tier campus network design. Readers will also learn the key functionality of a campus fabric architecture, such as Layer 3 routed access and the elimination of Spanning Tree Protocol.

Goals and Methods

The goal of this book is to illustrate how to implement Cisco SD-Access. Understanding the fundamental building blocks of a campus fabric architecture and how to design a software-defined campus will help readers determine the unique value that the Cisco SD-Access solution can bring to their organization.

This book can also help candidates prepare for the Cisco SD-Access portions of the Implementing Cisco Enterprise Network Core Technologies (ENCOR 350-401) certification exam, which is part of the CCNP Enterprise, CCIE Enterprise Infrastructure, CCIE Enterprise Wireless, and Cisco Certified Specialist – Enterprise Core certifications.

Who Should Read This Book?

The target audience for this book is network professionals who want to learn how to design, implement, and adopt Cisco SD-Access in their environment. This book also is designed to help readers learn how to manage and operate their campus network by leveraging Cisco DNA Center.

Candidates who are looking to learn about Cisco SD-Access as it relates to the ENCOR 350-401 exam will also find the necessary best practices and use case information valuable.

How This Book Is Organized

Although you could choose to read this book cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more experience with. Chapter 1 provides an overview of network automation, which is at the pinnacle of most conversations these days. Chapter 1 also covers some of the most common benefits of using automation in the campus networking environment. The dichotomy of using network automation is continuing to maintain and operate the network in a manual fashion. Chapters 2 through 9 are the core chapters and can be read in any order. If you do intend to read them all, the order in the book is an excellent sequence to follow.

Book Structure

The book is organized into nine chapters:

- **Chapter 1, "Today's Networks and the Drivers for Change":** This chapter covers the most common trends and challenges seen in the campus area of the network. This chapter also describes some of the benefits and key capabilities of automation in general, as well as the associated return on investment in terms of time and risk.
- **Chapter 2, "Introduction to Cisco Software-Defined Access":** This chapter discusses the need for software-defined networking, emphasizes the importance of security in IT networks, introduces network access control, and describes the value of segmentation using Cisco TrustSec and Cisco Identity Services Engine.
- **Chapter 3, "Introduction to Cisco DNA Center":** This chapter covers network planning and deployment trends, past and present, provides a brief history of automation tools, and introduces Cisco DNA Center and its core concepts.
- **Chapter 4, "Cisco Software-Defined Access Fundamentals":** This chapter introduces the basics of Cisco Software-Defined Access design, components, and best practices, along with the typical workflow to build and deploy a Cisco SD-Access fabric.
- **Chapter 5, "Cisco Identity Services Engine with Cisco DNA Center":** This chapter describes the integration of Cisco DNA Center and Cisco ISE, explains onboarding different types of endpoints securely using a phased approach, and examines the value of macro-segmentation and micro-segmentation and their use cases in Cisco SD-Access.
- **Chapter 6, "Cisco Software-Defined Access Operation and Troubleshooting":** This chapter goes deeper under the covers of Cisco SD-Access to explain the underlying technologies in the solution along with common fabric troubleshooting steps and examples.
- **Chapter 7, "Advanced Cisco Software-Defined Access Topics":** This chapter discusses multicast flows, Layer 2 flooding, and the extension of the Internet of Things (IoT) into Cisco SD-Access networks. It also includes various design considerations for Cisco SD-Access deployments and extending the policy to WAN and data center networks.
- **Chapter 8, "Advanced Cisco DNA Center":** This chapter discusses the deployment options for Cisco DNA Center itself, along with the various tools and solutions that are available independent of Cisco SD-Access.
- **Chapter 9, "Cisco DNA Assurance":** This chapter introduces the analytics offered by Cisco DNA Assurance, which include analytics regarding the health of clients, network devices, and applications. Assurance goes into detail with operational workflows and leverges a proactive approach to troubleshooting. Sensor-driven tests, insights offered by artificial intelligence and machine learning (AI/ML), as well as integration with third-party services such as ServiceNow for event tracking are useful for the IT operations team.

Chapter 1

Today's Networks and the Drivers for Change

This chapter covers the following topics:

- **Networks of Today:** This section covers the technologies that are driving changes in the networks of today.
- **Common Business and IT Trends:** This section covers the most common trends that are having a considerable impact on the network.
- **Common Desired Benefits:** This section examines the benefits and desired outcomes that organizations are looking for from a solution.
- **High-Level Design Considerations:** This section covers various aspects of network design and things that affect the deployment and operations of networks today.
- **Cisco Digital Network Architecture:** This section examines from a high level the benefits and drivers of Cisco DNA.
- **Past Solutions to Today's Problems:** This section covers the technologies used in the past and the challenges associated with them.
- **Introduction to Multidomain:** This section covers the value and benefits of a multidomain environment.
- **Cloud Trends and Adoption:** This section covers the trends and challenges of cloud adoption.

Networks of Today

The IT industry is constantly changing and evolving. As time goes on, there is an ever-increasing number of technologies putting a strain on the network. New paradigms are formed as others are being shifted away from. New advances are being developed and adopted within the networking realm. These advances are being developed to provide faster innovation and the ability to adopt relevant technologies in a simplified way.

This requires the need for more intelligence and the capability to leverage the data from connected and distributed environments such as the campus, branch, data center, and WAN. Doing so allows for the use of data in interesting and more powerful ways than ever seen in the past. Some of the advances driving these outcomes are

- Artificial intelligence (AI)
- Machine learning (ML)
- Cloud services
- Virtualization
- Internet of Things (IoT)

The influx of these technologies is putting a strain on the IT operations staff. This strain comes in the form of requiring more robust planning, agreed-upon relevant use cases, and detailed adoption journey materials for easy consumption. All these requirements are becoming critical to success. Another area of importance is the deployment and day-to-day operations of these technologies as well as how they fit within the network environment. Disruption to typical operations is more immanent with regard to some of these technologies and how they will be consumed by the business. Other advances in technology are being adopted to reduce cost of operations and to reduce complexity. Every network, to some degree, has inherent complexity. Having tools that can help manage this complexity is becoming a necessity these days.

Automation is something that many in the IT industry are striving for, because the networks of today are becoming more and more complicated. Often organizations are operating with a lean IT staff and a flat or diminishing IT budget and are struggling to find ways to increase the output of what the network can do for the business. Another driver for the adoption of these technologies is to improve the overall user experience within the environment. This includes enabling users to have the flexibility and capability to access any business-critical application from anywhere in the network and ensuring that they have an exceptional experience when doing so. In addition to improving user experience, the IT operations staff is searching for ways to simplify the operations of the network.

There are many inherent risks associated with manually configuring networks. There is risk in the form of not being able to move fast enough when deploying new applications or services to the network. Risk could also be seen as misconfigurations that could cause an outage or suboptimal network performance, resulting in impacting business operations and potentially causing financial repercussions. Finally, there is the risk that the business itself is relying on the network for some business-critical services and that they might not be available due to the IT operations staff not being able to keep up with the demand of the business from a scale perspective. According to a Cisco Technical Assistance Center (TAC) survey taken in 2016, 95 percent of Cisco customers are performing configuration and deployment tasks manually in their networks. The survey also stated that 70 percent of TAC cases created are related to misconfigurations. This means that typos or incorrectly used commands are the culprit for a majority of issues seen in the network environment. This is where automation shines. Having the capability to signify the intent of the change that needs to be made, such as deploying quality of service (QoS) across the network, and then having the network automatically configure it properly, is an excellent example of automation. This accomplishes configuring services or features with great speed and is a tremendous value to the business. Simplifying operations and reducing human error ultimately reduces risk.

A simple analogy for network automation would be to think of an automobile. The reason most people use an automobile is to meet a specific desired outcome. In this case, it would be to get from point A to point B. An automobile is operated as a holistic system, not a collection of parts that make up that system, as depicted in Figure 1-1. For example, the dashboard provides the driver all the necessary information regarding how the vehicle is operating and the current state of the vehicle. When the driver wants to use the vehicle, certain operational steps are required to do so. The driver simply signifies the intent to drive the car by putting it in gear and using the system to get from point A to point B.

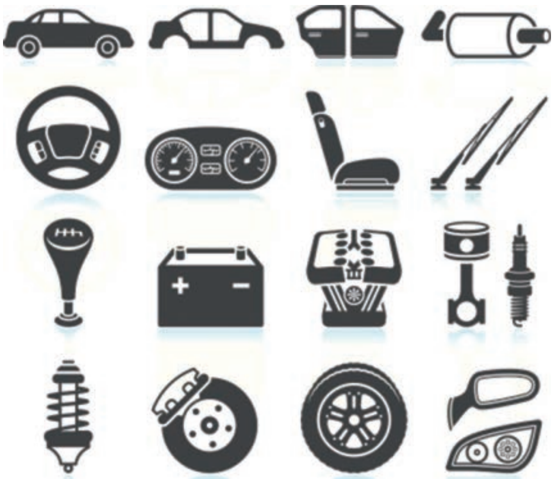


Figure 1-1 *Automobile as a System (Image Courtesy of Bubaone/Getty Images)*

Why can't networks be thought of in the same way? Thinking of a network as a collection of devices, such as routers, switches, and wireless components, is what the IT industry has been doing for over 30 years. The shift in mindset to look at the network as a holistic system is a more recent concept that stems from the advent of network controllers—the splitting of role and functionality from one another. The most common description of this is separating the control plane from the data plane. Having a controller that sits on top of the rest of the devices, so to speak, gives the advantage of taking a step back and operating the network as a whole from a centralized management point. This is analogous to operating an automobile from the driver's seat versus trying to manage the automobile from all the pieces and components that it is derived from. To put this in more familiar terms, think of the command-line interface (CLI). The CLI is not designed to make massive-scale configuration changes to multiple devices at the same time. Traditional methods of managing and maintaining the network aren't sufficient to keep up with the pace and demands of the networks of today. The operations staff needs to be able to move faster and simplify all the operations and configurations that have traditionally gone into networking. Software-defined networking (SDN) and controller capabilities are becoming areas of focus in the industry and are evolving to a point where they can address the challenges faced by IT operations teams. Controllers offer the ability to manage the network as a system, which means policy management can be automated and abstracted. This provides the capability of supporting dynamic policy changes versus its predecessor of manual changes of policy and configurations on a device-by-device basis when something requires a change within the environment.

Common Business and IT Trends

Traditional networking infrastructure was deployed when the security perimeter was well defined. Most applications were low bandwidth, and most content and applications resided in centralized corporate data centers. Today, enterprises have very different requirements. High-bandwidth, real-time, and big-data applications are pushing capacity limits of the network. In some cases, the majority of traffic is destined for the Internet or public cloud, and the security perimeter as it existed in the past is quickly disappearing. This is due to surge in bring your own devices (BYOD), cloud computing, and IoT. The downside and risks of staying status quo are significant, and technological innovation has failed to comprehensively address the problem. There has been a huge increase in the use of Software as a Service (SaaS) and Infrastructure as a Service (IaaS) offerings. It seems as if more applications are moving to the cloud each day. The adoption of solutions like Microsoft Office 365, Google Apps, Salesforce.com (SFDC), and other SaaS-based productivity and business applications is putting a strain on the network. This includes keeping the applications performing to the best of their ability in order to ensure that users have the best possible experience. The following list contains some of the most common trends occurring in the IT industry:

- Applications are moving to the cloud (private and public).
- Mobile devices, BYOD, and guest access are straining the IT staff.
- High-bandwidth applications are putting pressure on the network.
- Wireless-first connectivity is becoming the new normal.
- Demand for security and segmentation everywhere makes manual operations difficult.
- IoT devices often require access to the IT network.

The number of mobile devices in the campus and remote environments that are accessing these applications and the Internet as a result of BYOD and guest services is rapidly increasing. The additional load of traffic resulting from all of these devices, as well as trends such as IoT, is putting an additional strain on the network—especially in the wireless LAN. In addition to everything mentioned, interactive video has finally become the new voice from a popularity perspective. Converging voice and data services was an important transition. However, when it comes to video, today's networks not only have to account for optimized QoS handling for video applications, but also need to address the high-bandwidth, latency-sensitive applications that users are demanding. Traditionally, supporting these technologies was not easy, and implementing them required many manual configurations prior to deployment. This also led to additional complexity in the network environment.

With the business and IT trends covered thus far still in mind, it is important to translate these trends into real challenges that organizations are facing and put them into IT vernacular. As mentioned previously, the network is encountering pressure like never before. This is forcing IT teams to look for ways to alleviate that pressure. Organizations are also looking for ways to improve the overall user and application experience with what they currently own while also driving cost down. Lack of control over visibility and application performance, and keeping up with the ever-growing security attack surface are also contributing to organizations looking for a better way forward. In addition, organizational silos have caused many organizations to not be able to achieve the benefits from some of these newer technologies. Breaking down silos to work toward a common goal for the business as a whole is required for the business to take full advantage of what some of these software-defined advancements have to offer.

Common Desired Benefits

This section covers some of the most common benefits that organizations are looking for from their campus network. Designing and deploying the next-generation campus network is about taking advantage of some very useful benefits and the impact that they have on the network environment and overall user experience. Each of the benefits discussed is listed here:

- Prioritize and secure traffic with granular control
- Reduce costs and lower operational complexity
- Simplify troubleshooting with root cause analysis
- Provide a consistent high-quality user experience
- Implement end-to-end security and segmentation
- Deploy devices faster

Networks of today cannot scale at the speed necessary to address the changing needs that organizations require. Hardware-centric networks are traditionally more expensive and have fixed capacity. They are also more difficult to support due to the box-by-box configuration approach, siloed management tools, and lack of automated provisioning. Conflicting policies between domains and different configurations between services make today's networks inflexible, static, expensive, and cumbersome to maintain. This leads to the network being more prone to misconfigurations and security vulnerabilities. It is important to shift from connectivity-centric architecture to application- or service-centric infrastructure that focuses on user experience and simplicity.

The solution required to support today's cloud-enabled enterprise needs to be complete and comprehensive. It should be based on the software-defined approach mentioned earlier by leveraging the controller concept. The solution must also include a robust set of capabilities that reduces cost and complexity and promotes business continuity and rapid innovation. These capabilities should include the separation of the management plane, control plane, and data plane, which provides more horizontal scaling capabilities and the security of knowing where the data is at all times.

The solution should provide various consumption models, such as some components being hosted in the cloud and some components being managed on premises, with complete redundancy between the two. The solution must also provide a complete set of network visibility and troubleshooting tools that are accessible from a single place. Having this type of solution would assist in providing the following business outcomes and use cases:

- Faster device deployment with no operational interaction
- Complete end-to-end network segmentation for enhanced security and privacy
- Increased LAN performance
- Seamless host mobility
- Better user experience

All of the things mentioned thus far are critical in terms of what organizations are demanding to drive their network to becoming an asset that truly sets the organizations apart from their industry peers. Many organizations rely on the network to function at its best to provide value and competitive differentiation so their organizations can excel. This is what is driving this industry to these types of technologies. This reliance is also why the industry has increased the speed of adoption and deployment of these solutions.

High-Level Design Considerations

Considering the complexity of a majority of the networks out there today, they can be classified in a couple categories such as redundant and nonredundant. Typically, redundancy leads to increased complexity. Often, the simplest of networks do not plan for failures or outages and are commonly single-homed designs with multiple single points of failure. Networks can contain different aspects of redundancy. When speaking strictly of the campus LAN portion of the environment, it may include redundant links, controllers, switches, and access points. Table 1-1 lists some of the common techniques that are introduced when dealing with redundancy.

Table 1-1 *Common Redundancy Techniques*

Redundant Links	Redundant Devices
Administrative distance	Redistribution
Traffic engineering	Loop prevention
Preferred path selection	Preferred path selection
Prefix summarization	Advanced filtering
Filtering	

Many redundancy options are available, such as redundant links, redundant devices, EtherChannel, and so on. Having a visual of what some of these redundancy technologies look like is often helpful. One of these technologies is Cisco Virtual Switching System (VSS), which bonds switches together to look and act like a single switch. This helps put into context how the network will need to be configured and managed to support these types of redundancy options. The following are some of the benefits of VSS technology:

- Simplifies operations
- Boosts nonstop communication
- Maximizes bandwidth utilization
- Lowers latency

Redundancy can take many different forms. VSS is used for much more than just redundancy. It helps with certain scenarios in a campus design, such as removing the need for stretched VLANs and loops in the network. Figure 1-2 showcases an example of a campus environment before and after VSS and depicts the simplification of the topology.

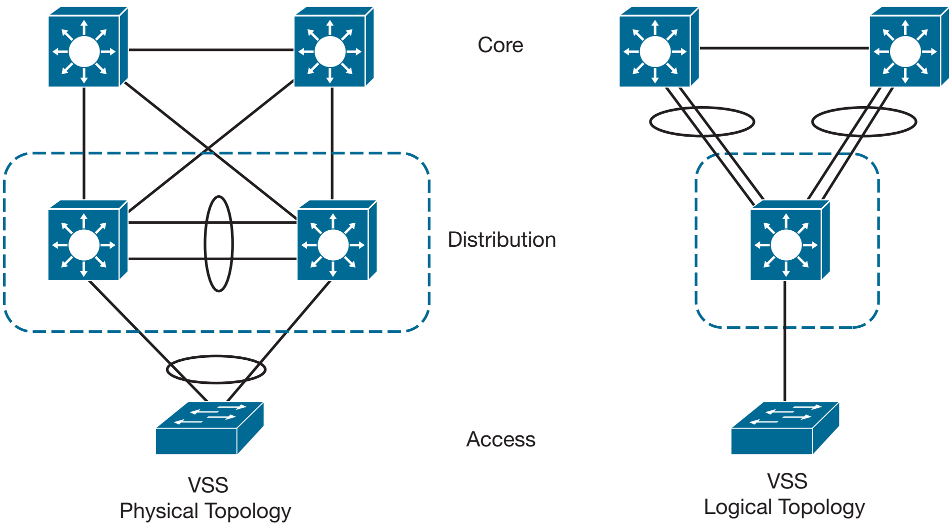


Figure 1-2 *VSS Device- and Link-Based Redundancy Options*

Outside of the complexity associated with redundancy, there are many other aspects of the network that cause complexity within a network environment. Some of these aspects can include things such as securing the network to shield it from malicious behavior, leveraging network segmentation to keep traffic types separate for compliance or governance reasons, and even implementing QoS to ensure optimal application performance and increase users' quality of experience. What further complicates the network is having to manually configure these options. The networks of today are too rigid and need to evolve. The industry is moving from the era of connectivity-centric network delivery models to an era of digital transformation. There is a shift required to transition to a digital transformation model. The shift is from hardware- and device-centric options to open, extensible, software-driven, programmable, and cloud-enabled solutions. Figure 1-3 depicts the transition in a simple summary. Relying more on automation to handle the day-to-day operational tasks and getting back time to focus on how to make the network provide value to the business is crucial to many organizations. This is delivered through policy-driven, automated, and self-optimizing capabilities. This provides closed-loop, automated service assurance that empowers network operations staff to transition from a reactive nature to a more proactive and predictive approach. Freeing up more of the operations staff's time should enable them to focus on more strategic initiatives within the business.

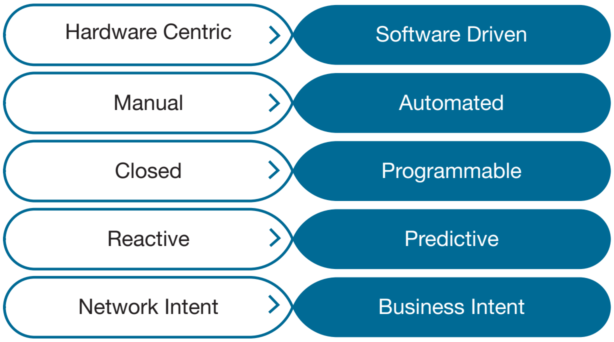


Figure 1-3 *Digital Transformation Transition*

Intent-based networking (IBN) is taking the IT industry by storm. The concept revolves around signifying the intent of the business and automatically translating that intent into the appropriate corresponding networking tasks. This is a circular logic in that it captures the intent of the business and IT staff and then translates that intent into the appropriate policies that are required to support the business. Once the policies are created, the next step is to orchestrate the configuration of the infrastructure. This includes both physical and virtual components. This then kicks off the final step, which is providing assurance, insights, and visibility to ensure the network is functioning properly. Because this is a loop in a sense, the logic uses continuous verification and supplies any corrective actions that are necessary to fix or enhance the network's performance. Figure 1-4 illustrates the intent-based networking model.

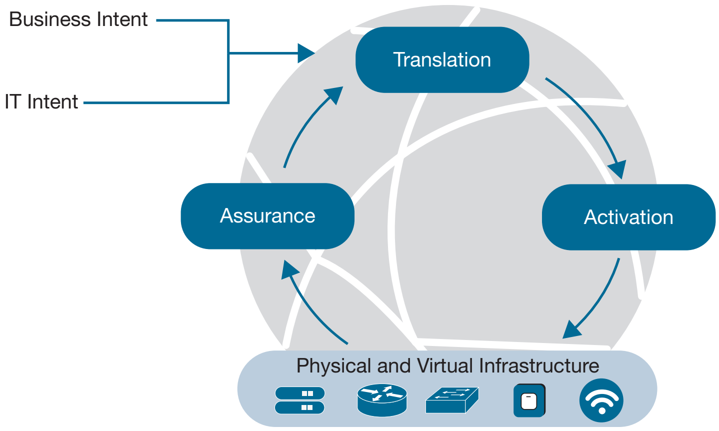


Figure 1-4 *Intent-Based Networking*

Analytics and insights are absolutely critical to networks of today. Typical network management systems (NMSs) do not provide the necessary information to resolve issues in a quick and efficient manner. They are reactive in nature and don't supply the predictive monitoring and alerting that organizations require. Simple Network Management Protocol (SNMP) Traps and SYSLOG messages are valuable but haven't been used as well as they could be. Reactive notifications mean that the issue or fault has already happened and don't prevent any impact to the business. Often, there are false positives or so many alerts that it is difficult to determine what information should be acted upon or ignored completely. Traditionally, the network operations workflow has been similar to the following:

1. Receive an alert or helpdesk ticket.
2. Log in to the device(s) to determine what happened.
3. Spend time troubleshooting.
4. Resolve the issue.

The days are over of hunting around and searching through log files and debugging traffic to determine what the issue is that has caused an outage to the network. The amount of data that runs through these networks and has to be sorted through to chase down an issue is exponentially increasing. This is leading to the manual sifting through information to get to the root cause of an issue being extremely more difficult than ever before. Organizations rely on information relevant to what they are looking for; otherwise, the data is useless. For example, if a user couldn't get on the wireless network last Tuesday at 3 p.m., and the logs are overwritten or filled with non-useful information, how does this help the network operations staff troubleshoot the issue at hand? It doesn't. This wastes time, which is one of the most precious resources for network operations staff. The dichotomy of this is using analytics and insights to help direct network operators to the right place at the right time to take the right action. This is part of what Cisco DNA Assurance does as part of intent-based networking.

Problem isolation is much easier within an intent-based network because the entire network acts as a sensor that provides insights into the failures that are happening in the network. The network also has the capability to have a holistic view of the network from a client perspective. From a wireless perspective alone, this can provide information such as failure reasons, received signal strength indicator (RSSI), and onboarding information.

One of the most time-draining parts of the troubleshooting process is trying to replicate the issue. The previously mentioned issue of a user not being able to get on the network last Tuesday at 3 p.m. would be very difficult to replicate. How would anyone know what possibly was going on last Tuesday at 3 p.m.? In reality, the only traditional way to know what was going on from a wireless perspective was to have constant packet captures and spectrum analyzers running. Due to cost, space, and not knowing where the issue may arise, this is not a practical approach. What if instead there was a solution that could not only act as a DVR for the network but also use streaming telemetry information such as NetFlow, SNMP, and syslog and correlate the issues to notify the network operations staff of what the issue was, when it happened—Even if it happened in the past? Imagine the network providing all this information automatically. Additionally, instead of having Switched Port Analyzer (SPAN) ports configured across the campus with network sniffers plugged in everywhere in hopes of capturing the wireless traffic when there is an issue, imagine the wireless access points could detect the anomaly and automatically run a packet capture locally on the AP that would capture the issue. All these analytics could provide guided remediation steps on how to fix the issue without requiring anyone to chase down all the clues to solve the mystery. Fortunately, that solutions exists: Cisco DNA Assurance can integrate using open APIs to many helpdesk ticketing platforms such as ServiceNOW. The advantage of this is that when an issue happens in the network, Cisco DNA Assurance can automatically detect it and create a helpdesk ticket, add the details of the issue to the ticket as well as a link to the issue in Assurance, along with the guided remediation steps. That means when the on-call support engineer gets the call at 2 a.m., she already has the information on how to fix the issue. Soon, automatic remediation will be available, so the on-call person won't have to wake up at 2 a.m. when the ticket comes in. This is the power of Assurance and intent-based networks.

Cisco Digital Network Architecture

Cisco Digital Network Architecture (DNA) is a collection of different solutions that make up an architecture. It is the Cisco intent-based network. Cisco DNA is composed of four key areas: WAN, campus, data center, and cloud edge. Each area has its own Cisco solutions that integrate with each other: Cisco Software-Defined WAN (Cisco SD-WAN), Cisco Software-Defined Access (Cisco SD-Access), Cisco Application Centric Infrastructure (Cisco ACI), and Cisco Secure Agile Exchange (SAE). Each area is built with security ingrained in each solution. Figure 1-5 illustrates the pillars of Cisco DNA. At the center, Cisco DNA is powered by intent, informed by context, constantly learning, and constantly protecting. This is what translates the business intent into network policy, provides constant visibility into all traffic patterns, leverages machine learning at scale to provide increasing intelligence, and enables the network to see and predict issues and threats so the business can respond faster.

The increased use of cloud services and mobile devices is creating IT blind spots. This industry demands a new holistic approach to security. Security is at the core of Cisco DNA. Cisco offers a full life cycle of on-premises and cloud-hosted solutions to maximize protection for organizations. Because Cisco can focus on all aspects of security, this lowers complexity by reducing to one the number of security vendors required to protect the business. Cisco DNA can turn the entire network into a sensor to detect malicious traffic and anomalies in behavior. Figure 1-6 shows the different areas of security that Cisco provides solutions for.

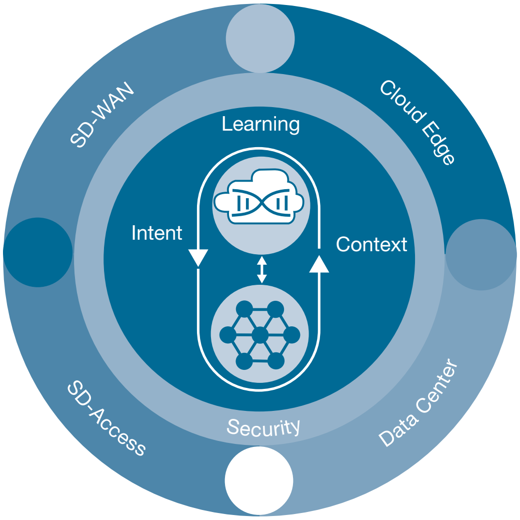


Figure 1-5 *Cisco Digital Network Architecture (DNA)*

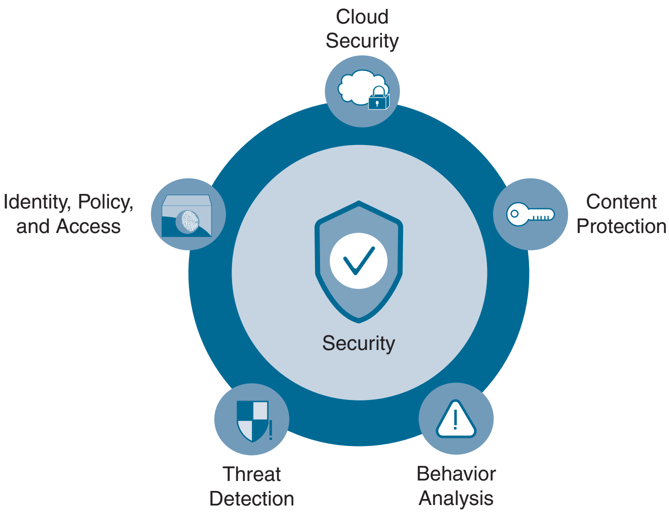


Figure 1-6 *Cisco Security Overview*

Cisco Stealthwatch can baseline the network and provide anomaly detection when something changes. This even includes detecting changes in traffic or user behavior. A great example of this is when a user typically uses an average amount of bandwidth within the network to do her daily job tasks. If all of a sudden the user starts downloading gigabytes' worth of data and sending it to another machine in another country, Stealthwatch considers this an anomaly. This doesn't necessarily mean the user is being malicious or stealing company data; it could be that the user's machine has been compromised and malware is attacking the network. In either case, Stealthwatch would be able to detect this and inform the IT operations staff to take action. Automated network segmentation can address this type of challenge to ensure that the users and networks are in compliance. Taking this innovation a step further, the Cisco Catalyst 9000 Series switches have the capability to detect malware and other malicious threats within encrypted traffic. This is called Cisco Encrypted Traffic Analytics (ETA). This is unique to Cisco and is one of the most advanced forms of security protection available today. Combining this with all the telemetry and visibility that the network can provide, it greatly reduces the risk and potential impact of threats to the network. It is important to note that the power of Cisco DNA is that all of these technologies across all of these pillars work in concert. Security is ingrained in everything Cisco offers; it is not an afterthought or something that rides on top of the network—security *is* the network. Figure 1-7 depicts the Cisco stance on security and how it fits within the network environment. It illustrates that security is just as critical as the network itself. Providing the most robust network that can provide value to the business and enhance users' application experience in a secure and agile fashion is essential to many organizations.

Figure 1-7 *Security in Everything*

Past Solutions to Today's Problems

Over the years, demands on the network have steadily increased, and the IT industry has adapted to these demands. However, this doesn't mean that the industry has adapted quickly or properly. Networks only exist to carry applications and data. The methods of how these applications and data have been handled have also been in constant flux. From a design perspective, the mechanisms implemented in the network ultimately depend on the outcome the business is trying to achieve. This means that the mechanisms aren't always best practice or validated designs. The configurations of these devices are often ad hoc in nature and usually include point-in-time fixes for issues that arise in the network that need to be addressed.

Spanning-Tree and Layer 2–Based Networks

One of the most common technologies that gets a lot of notoriety is Spanning Tree. Spanning Tree was designed to prevent loops in the Layer 2 network. However, it can cause a tremendous amount of problems in the network if not tuned and managed properly. There are many settings and configuration techniques for Spanning Tree as well as multiple versions that provide some variation of what the protocol was designed to do. Table 1-2 lists the many versions or flavors of Spanning Tree and their associated abbreviations.

Table 1-2 *Spanning Tree Versions*

Type of Spanning Tree	Abbreviation
Legacy Spanning Tree Protocol	STP
Per-VLAN Spanning Tree	PVST
Per-VLAN Spanning Tree Plus	PVST+
Rapid Spanning Tree Protocol	RSTP
Rapid Per-VLAN Spanning Tree Plus	RPVST+
Multiple Spanning Tree	MST

Spanning Tree is often used in three-tier campus architectures that rely on Layer 2 distribution and access layers, with routing typically done at the distribution block. This entirely depends on design, of course, but this is the usual place for Spanning Tree. First hop redundancy protocols (FHRPs) are used for each subnet and are configured to provide gateway information for the local subnets and aid in routing the traffic to its destination. The following are examples of first hop redundancy protocols:

- Hot Standby Routing Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Gateway Load Balancing Protocol (GLBP)

Prior to the advent of Layer 3 routed access, Spanning Tree was also primarily used in Layer 2 networks that had stretched VLANs to support mobile wireless users. This was because wireless users required the capability to roam anywhere in the campus and maintain the same Service Set Identifier (SSID), IP address, and security policy. This was necessary due to the reliance on IP addresses and VLANs to dictate which policy or access list was associated to which wired or wireless user. However, there were inherent limitations of Spanning Tree, such as only being able to use half the bandwidth of a pair of redundant links. This is because the other path is in a blocked state. There are, however, many different ways to manipulate this per VLAN or per instance, but this is still the case for Spanning Tree. Other drawbacks are the potential for flooding issues or blocked links causing an outage in the network. This impacts business continuity and disrupts users, making it difficult to get the network back online in a quick fashion. Some Spanning Tree outages can last for hours or days if the issue is not found and remedied.

Figure 1-8 illustrates a typical three-tier campus network architecture design that leverages Spanning Tree and HSRP, showing that there are certain links that are unusable because Spanning Tree blocks links to avoid a looped path within the network.

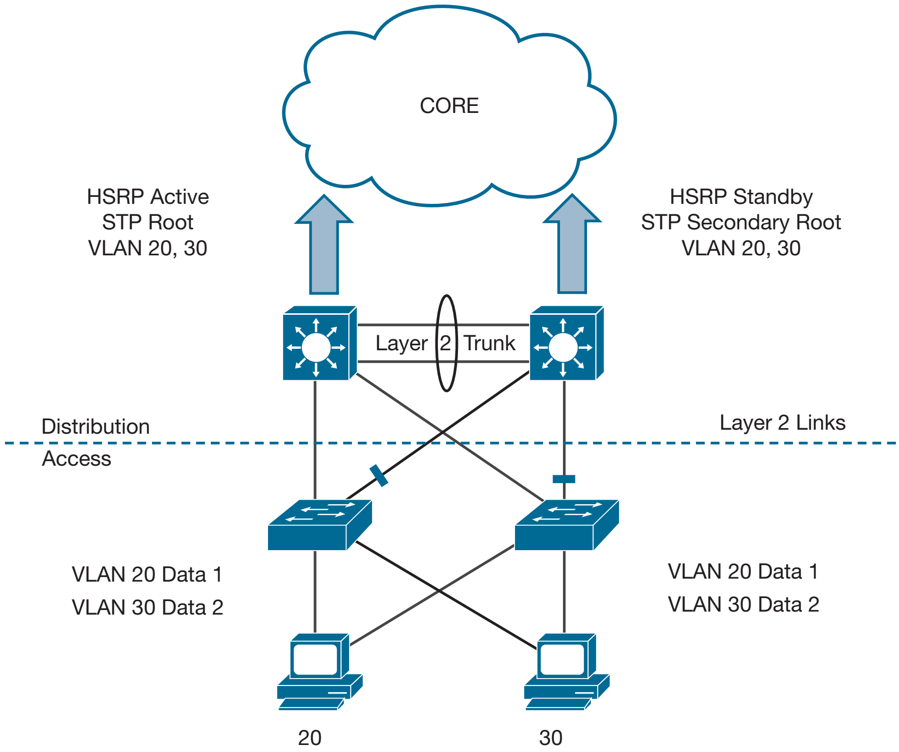


Figure 1-8 *Spanning Tree Example*

With the advent of Layer 3 routed access, Spanning Tree is no longer necessary to prevent loops because there is no longer a Layer 2 network. However, Layer 3 routed access introduced another set of issues that needed to be addressed. There is still the issue of security policy relying on IP addressing. In addition, now that VLANs are not being stretched across the network using trunking, wireless networks have to change how they operate. This means that wireless SSIDs have to map to subnets, and if a user moves from one access point on an SSID and goes to the same SSID in another area of the network on a different access point, it is likely that their IP address would change. This means there has to be another access list on the new subnet with the same settings as the access list on the previous subnet; otherwise, the user's security policy would change. Imagine the overhead of having to configure multiple access lists on multiple subnets. This is how networks were traditionally configured. The amount of manual configuration, potential for misconfiguration, and time wasted are just some of the caveats of this type of network design. Figure 1-9 depicts a Layer 3 routed access network.

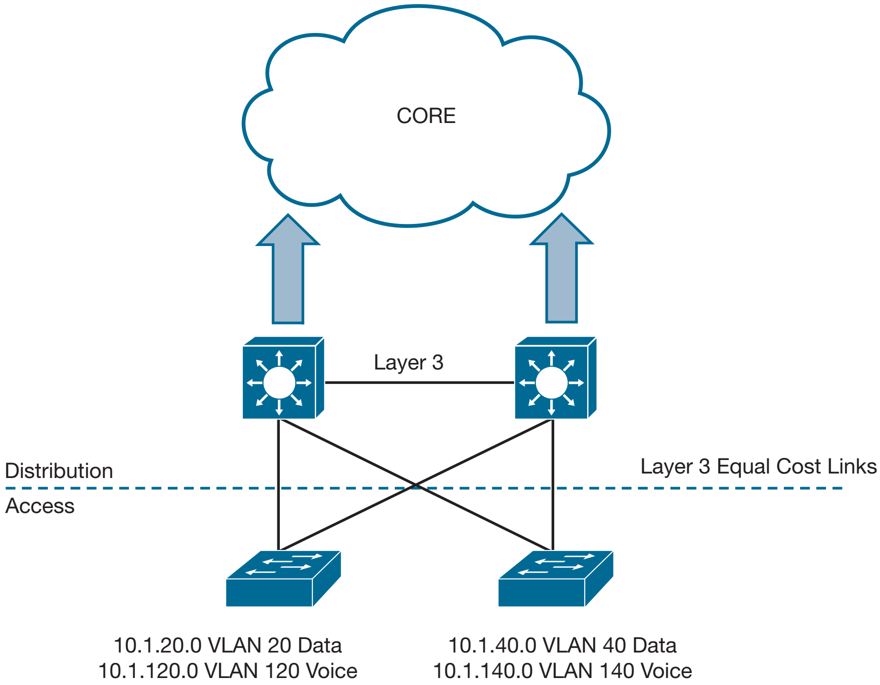


Figure 1-9 *Routed Access Example*

Layer 3 routed access is also very prominent in the data center environment. This is due to all the benefits of moving to a Layer 3 routed access model versus a Layer 2 network. The following is a list of benefits to using a routed access network:

- Increased availability
- Reduced complexity
- Simplified design
- Removal of Spanning Tree

As mentioned earlier in this chapter, real-time and interactive video applications are becoming more mainstream, and organizations expect their users to have the capability to connect from anywhere at any time. The campus network must be available at all times to support this type of business case. Routed access leverages point-to-point links, which not only reduces the amount of time it takes to recover from a direct link failure, but simplifies the design by relying only on a dynamic routing protocol (versus Layer 2 complexities, Spanning Tree, and Layer 3 routing protocols). Coupled with all links in the environment now being active and forwarding traffic, there is a large gain in bandwidth and faster failure detection with point-to-point links versus Layer 2. The industry is demanding networks that include ultra-fast, low-latency, high-bandwidth links that are always available and that are able to scale to meet the demands of the organizations that are using them. Figure 1-10 illustrates the difference between Layer 2– and Layer 3–based campus designs.

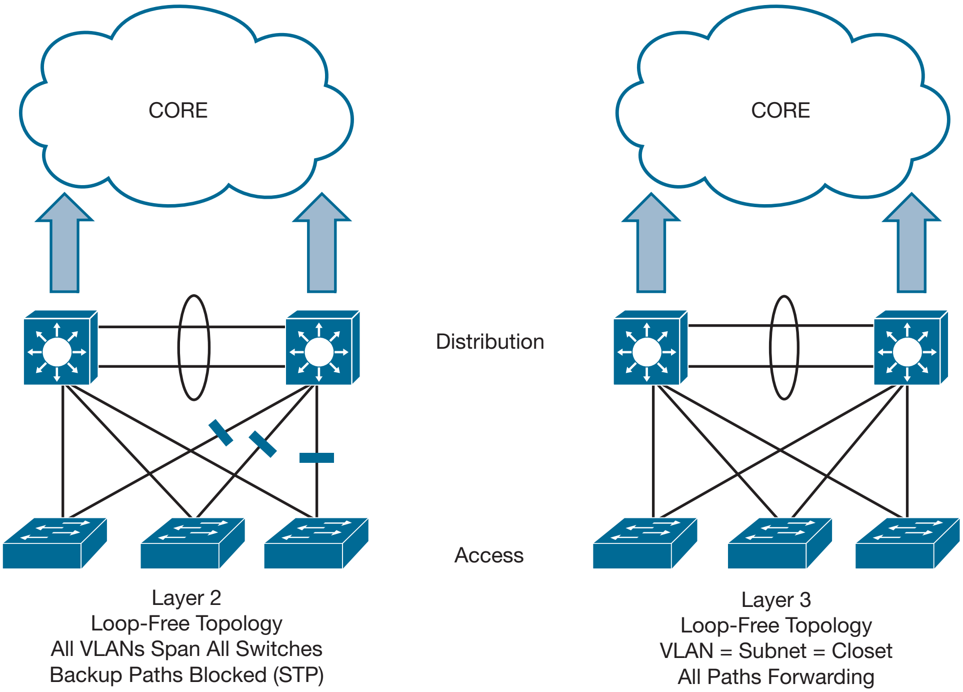


Figure 1-10 *Layer 2 Versus Layer 3 Campus Design*

Introduction to Multidomain

A common trend that is arising in the IT industry is to generate and store data in many areas of the network. Traditionally, a majority of the data for a business was stored in a centralized data center. With the influx of guest access, mobile devices, BYOD, and IoT, data is now being generated remotely in a distributed manner. In response, the industry is shifting from data centers to multiple centers of data. That being said, simple, secure, and highly available connectivity is a must to allow for enhanced user and application experience. The other big piece to multidomain is having a seamless policy that can go across these multiple centers of data. An example of this is policy that extends from the campus environment across the WAN and into the data center and back down to the campus. This provides consistency and deterministic behavior across the multiple domains. Figure 1-11 illustrates a high-level example of sharing policy between a campus branch location and a data center running Cisco Application Centric Infrastructure (ACI).

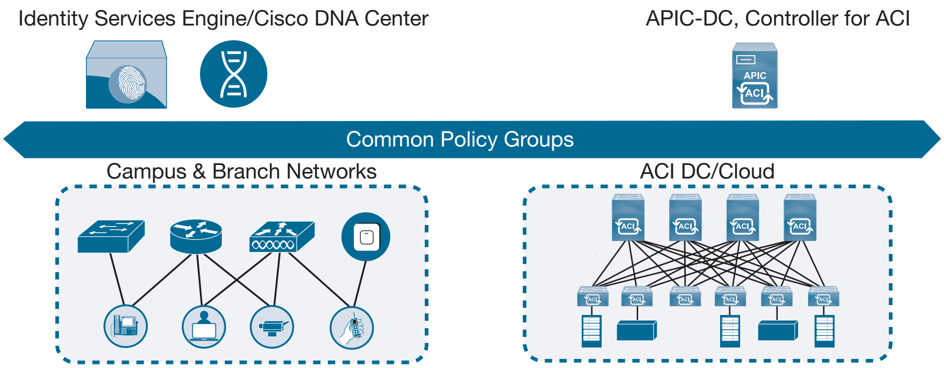


Figure 1-11 *High-level Multidomain Example*

In future evolutions of multidomain, the common policy will extend from the campus across the Cisco Software-Defined WAN (SD-WAN) environment to Cisco ACI running in the data center and back down to the campus, providing end-to-end policy and management across all three domains. This will provide the capability to leverage things like application service-level agreements (SLAs) from the data center to the WAN and back, ensuring that the applications are performing to the best of their ability across the entire network. It will also relieve strain on the WAN and provide a better user experience when using the applications. Figure 1-12 shows a high-level example of what this could look like from an overall topology perspective.

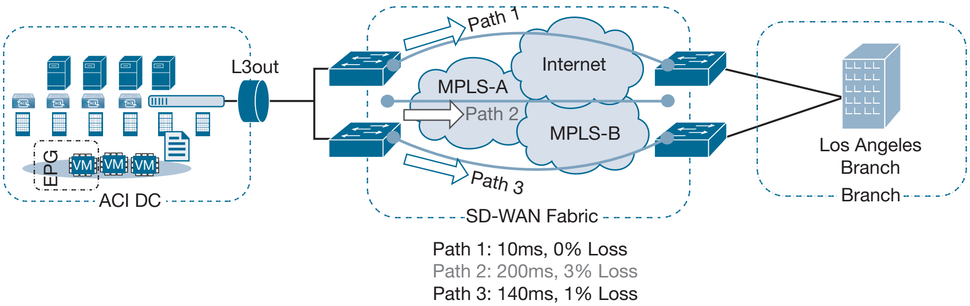


Figure 1-12 *High-level Multidomain with ACI and SD-WAN Example*

Multidomain offers the capability to have the network operate as a holistic system, as mentioned previously in this chapter. This takes intent-based networks to the next level by taking policy across all domains for a seamless application experience. This also implements security everywhere and provides complete granularity in terms of control and operations. Looking at multidomain from another aspect, the Cisco Software-Defined Access solution can share policy with the Cisco SD-WAN solution as well. This is powerful because the policies that control security, segmentation, and application performance can be enforced across the entire network environment. This means that the user and application experience is congruent across the campus LAN and WAN. Tying both domains together is what delivers the capabilities to protect the applications and ensure that the business outcomes organizations are striving for are being met. Figure 1-13 illustrates a high-level multidomain design with Cisco DNA Center, Cisco vManage, Cisco SD-Access, and Cisco SD-WAN.

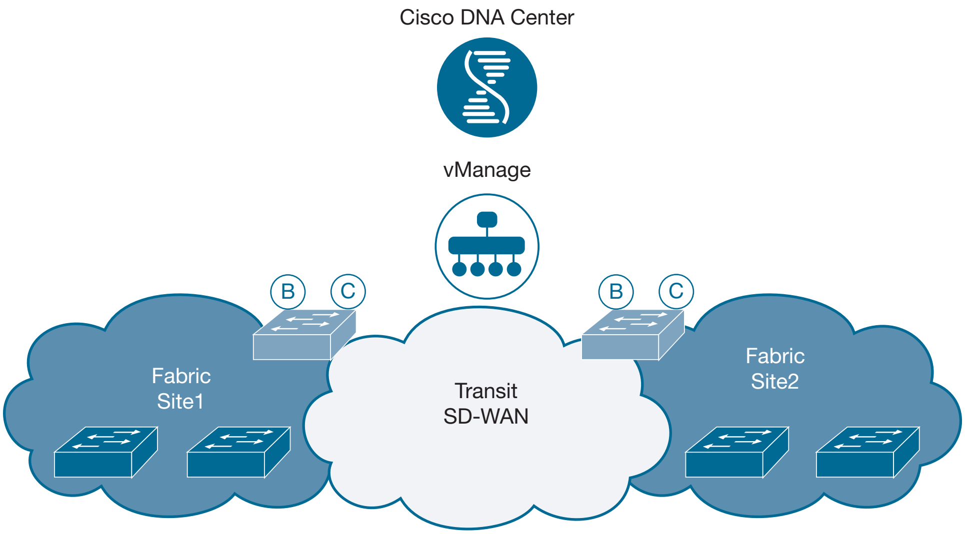


Figure 1-13 *High-level Multidomain with Cisco SD-Access and SD-WAN Example*

Cloud Trends and Adoption

Cloud adoption has been taking the industry by storm. Over the years, the reliance on cloud computing has grown significantly, starting with music, movies, and storage and moving into SaaS and IaaS. Today, there are many aspects of organizations that run in the cloud, such as application development, quality assurance, and production. To make things even more complicated, companies are relying on multiple cloud vendors to operate their business, resulting in unique sets of polices, storage capacity requirements, and overall operations skills on a per-vendor basis. Companies are struggling with things such as shadow IT and backdoor applications in their environment. Shadow IT is when lines of business (LoB) are going to cloud providers on their own, without any knowledge or guidance from the IT departments, and spinning up applications on demand in the cloud. This causes major concerns from a security and privacy perspective. In addition, the potential loss of confidential information or intellectual property could damage the brand and reputation of the business. The risks are significant.

Furthermore, the applications in the cloud, whether legitimate production applications or applications that are currently in development, still require certain levels of priority and treatment to ensure the applications are being delivered properly to the users who consume them. This is where some of the capabilities of the next-generation campus network can help to ensure that the applications are being treated appropriately and the experience for the users is adequate. Figure 1-14 illustrates the demand on the campus LAN and WAN and how cloud applications are becoming critical to the operations of the business. The campus network has the shared responsibility of ensuring that the applications perform to the best of their ability and provide an exceptional user experience. The campus network also has to share the security burden to make sure that the appropriate users are accessing the applications and sharing information in the first place. This is where having a good segmentation and security policy is paramount.

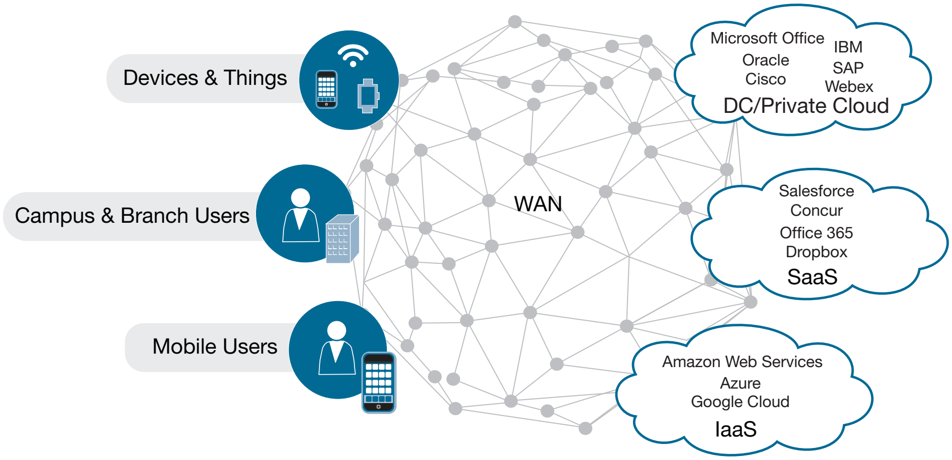


Figure 1-14 *Demand on LAN and WAN for Internet-based Applications*

The majority of the bandwidth that applications consume affects the WAN environment more than the campus LAN. This is due to the WAN links having a more finite amount of bandwidth versus the high-speed bandwidth links seen within a campus environment. Having direct Internet access in a branch can assist with alleviating some of this pressure. By being able to detect application performance through one or more direct Internet access circuits, the branch routers are able to choose the best-performing path based on the application-specific parameters. This helps offset the low-bandwidth WAN transport. If one of the links to the cloud application fails or has degradation in performance, the application can automatically fail over to another direct Internet link. This process is fully automated and requires no interaction from the network operations staff. Figure 1-15 shows this scenario with multiple direct Internet access links.

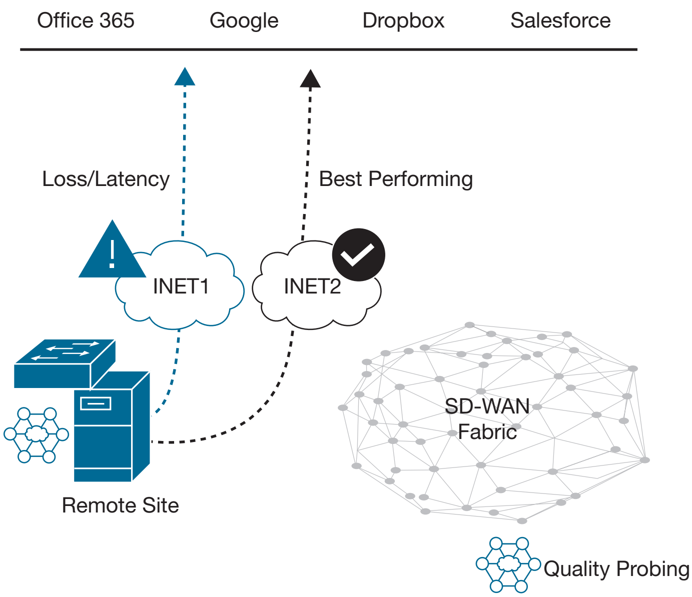


Figure 1-15 *Multiple Direct Internet Access Links to Cloud Applications*

Summary

This chapter provided a high-level overview of how the networks of today are causing challenges for organizations and their operations staff. It also covered the common business and IT trends that the industry is seeing and how they affects the networks of today. The overall benefits desired by organizations and their IT staff lead to the need to rethink the campus environment. Cloud applications and the influx of the amount of data within the network is causing strain on the network. This is causing organizations to look at ways to alleviate the pressure that is being put on the network and the organization as a whole. Security is no longer an afterthought; it is crucial to incorporate security into everything in the environment. This means that from concept to design to implementation, security must be thought of the entire way. The use cases introduced in this chapter will each be covered in depth in the upcoming chapters. Application performance, security, segmentation, improved user experience, redundancy, and resiliency are key drivers that point to an intent-based network infrastructure.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O