Solution overview Cisco public

The bridge to possible

Network Transformation Made Easy with Lab Validation

Executive Summary

Digital transformation is omnipresent, and no industry is immune from having to build next-generation networks rapidly. Deploying a software-defined solution across the wide area network, migrating to a newer virtual platform in the data center, upgrading the wireless network on campus, or enabling a new security policy for remote workers at scale, requires proper validation of the solution and technology.

The need to build solutions and enable capabilities rapidly has resulted in many organizations implementing half-baked solutions, leading to production-impacting poor user experience, lost productivity due to network downtime, and higher costs to remediate the issues. These effects are compounded by the increased risk of vulnerabilities and the associated attacks, due to suboptimal configurations. And while some vendors conduct testing for their specific products, it is vital to test solutions with multiple vendors to minimize compatibility and integration risks.

Today, increased network outages exist due to poor implementation caused by minimal or no validation of the changes. When it comes to business, time is of the essence, and practical implementation is essential for an organization to succeed. Making changes to the infrastructure based on validated information is more critical than ever.

While there are many options for an enterprise when enabling newer software, hardware, and features or rolling out innovative solutions, it is recommended that a thorough lab validation is conducted to minimize the risks with implementation.

Introduction

Organizations build and implement solutions leveraging multiple technologies to achieve digital transformation. As they go through the process of creating the next-generation architecture by planning, designing, and implementing modern technology solutions, one of the most critically overlooked phases is “validating” the solution or technology in a controlled environment. The failure to validate typically leads to delayed rollouts, network downtime, and suboptimal configurations resulting in an overall inferior performance of the network, exposure to security risks, and poor user experience.

In fact, according to Gartner: the cost of network downtime based on industry surveys is typically $5,600 per minute, which extrapolates to well over $300K per hour.

It is imperative to thoroughly validate the solutions and capabilities before implementing them in production. Testing the solutions in an automated fashion at scale helps businesses efficiently adopt newer solutions and technologies into the infrastructure cost-effectively. Furthermore, automating test cases offers the following benefits:

- **Efficiency:** Automated network tests save time and resources by running more test cases in a shorter amount of time.
- **Reliability:** Automated tests are executed reliably and consistently, especially in complex environments.
- **Scalability:** Automated tests offer flexibility to scale up or down as needed to cover various scenarios.

This paper will focus on lab validation, its importance, its numerous benefits, and a specific example of a large multi-national enterprise customer benefiting from the lab services delivered through the Cisco Solution Validation Services (SVS) Team.

Cisco SVS provides lab validation services to customers in several industries. With high proficiency in multiple solutions and technologies, SVS has helped numerous customers address their specific needs and challenges. The design and engineering teams can be assured of successful implementation by validating solutions in the lab and proactively identifying interoperability issues, software defects, scalability limits, performance, and more. Additionally, SVS offers thousands of predefined test cases to accelerate test cycles and expedite implementation.

While it is crucial to test the new solution, feature, or capabilities after implementation, this paper will highlight the analysis of validation and testing before implementing the solution in production.

Definition of Lab Validation

Lab validation is a process that is planned and executed in an organized fashion to test functional and nonfunctional requirements in a controlled environment. The validation could be as simple as certifying a newer product to replace end-of-life hardware or validating a solution that involves multiple technologies and products.

For instance, one example is replacing a distribution switch that aggregates multiple access layer switch in a campus to minimize the risks associated with newer hardware and software. Validating the hardware replacement in the lab helps identify potential issues and risks.

Or consider a scenario where there is a significant change in the topology of the network. It is vital to ensure all protocols, configurations, and failover scenarios work as expected before implementing them in production.

Suppose the enterprise security team must apply security policies to infrastructure devices like switches, routers, and firewalls. Testing the security policy in the lab and simulating traffic flows to ensure security policies are being enforced correctly will help avoid costly mistakes due to poor security policy rollout.

Although there are numerous other examples, it is evident that lab validation is a crucial factor in achieving a successful and error-free deployment of solutions and technologies.

Importance of Lab Validation

Validation of the solution is critical for an organization to implement the solution and technology successfully. Many enterprises spend their valuable time-solving problems but have yet to find preventative measures to avoid them.

Enterprises often need to understand the implications before attempting to make infrastructure changes. Lab validation can avoid risks such as unsuccessful maintenance windows leading to more downtime than planned, poor application and user experience, and additional time spent troubleshooting the issues.

Adoption of lab validation can ensure that the solution's functional and non-functional requirements, including hardware, software, protocols, and configurations, are functioning as designed. And by leveraging automation in the validation process, regression testing could be performed to ensure software upgrades do not have negative impacts, or network changes can be tested in a NetDevOps pipeline before applying them to production.

Benefits

The following are just a few of the many benefits of lab validation:

Proactive identification of issues: This is one of the most significant benefits of lab validation. The ability to proactively identify issues and develop a solution is far more valuable than implementing a non-tested configuration in the production environment and running into unplanned downtime.

Stakeholder approval process: Stakeholders need information to make a Go/No-Go decision with the proposed solution. Sharing lab validation results, including insights and risks, with stakeholders can help to make informed decisions.

Create awareness of the solution: While lab validation is not necessarily considered a training platform, organizations can create awareness and familiarity with the solution as it is ready to be implemented in production. The engineering and operations team can access the lab setup to review the design, configurations, and even display outputs to better understand the technologies.

Change advisory board: To ensure minimal or no impact on the production environment, organizations need detailed documentation of implementation or maintenance windows. By proactively leveraging lab testing and its results, the advisory board can assess the risk and approve or deny the request accordingly.

Implementation schedule: Build a realistic project schedule based on lessons learned from the lab validation and deliver a successful implementation.

Efficient adoption of changes: Anticipating changes, such as adding a capability or enabling a new feature during solution build and deployment, should be expected. Lab validation can help execute these changes with minimal or no risk in production.

Interoperability: Most networks have a hybrid solution in the environment—for instance, a load balancer solution interfacing with switches and firewalls from another vendor. Thoroughly testing interoperability in the lab before rolling out the solution can increase the chances of a successful implementation.

Availability: Infrastructure has become the foundation for users and applications to interact seamlessly. Organizations thrive on this interaction to grow the business and ensure their service is always available. Lab validation can help avoid poor execution and meet the organization's availability criteria.

Employee morale: Many times, maintenance windows executed after business hours require human intervention. Successful implementation leads to fewer maintenance windows and a positive impact on technical and non-technical teams, leading to higher employee satisfaction.

Customer Use Case

A multinational corporation with over 300+ branches, two data centers, and six carrier-neutral facilities across the globe was transforming into a modern and more digital infrastructure to meet its business outcomes. The goal was to build a controller-based solution for managing the network, provide a seamless experience to both wired and wireless users, and optimize traffic flow across the transport based on the application requirements.

The Cisco® Customer Experience (CX) team and the Account team developed an extensive architecture capable of supporting easy access to authorized network services from anywhere at any time, managing a high volume of traffic flows, and providing adequate security across the enterprise that met privacy, regulatory, and compliance requirements.

High-Level Architecture

The diagram below highlights the overall solution and technologies at an elevated level and focuses on all the components deployed in the lab validation. The goal is not to focus on the details of the solution but to focus on end-to-end validation with site types for campus, branches, Software-Defined Wide Area Networking (SD-WAN), and Spine Leaf Virtual Extensible Local Area Network (VxLAN) topology.

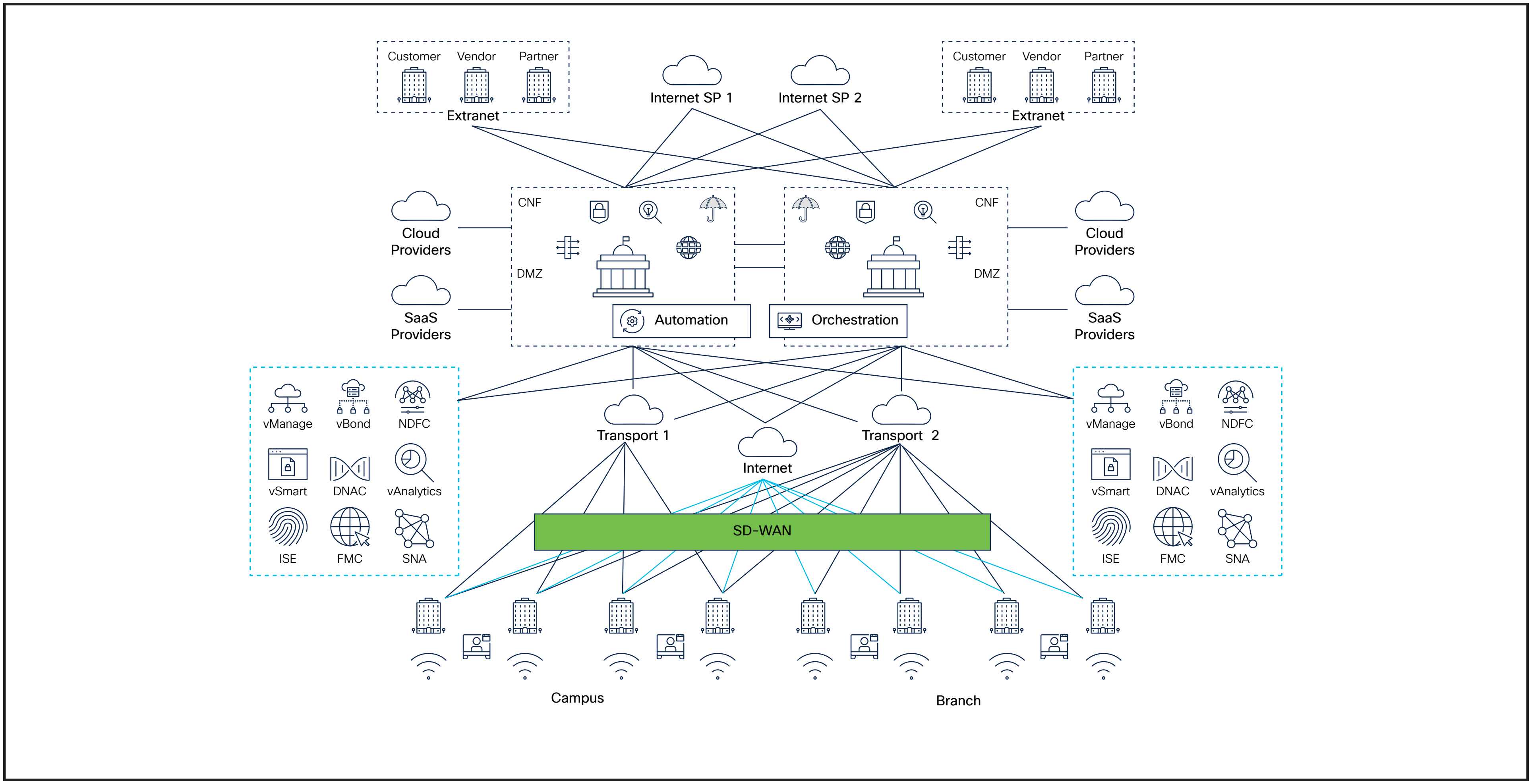


Figure 1. High-Level Architecture Diagram

The architecture included:

- Catalyst® 9Ks, Cisco IOS® XE–based wireless, and Cisco Digital Network Architecture Center (Cisco DNA Center™) in the campus.
- SD-WAN across the transport with vManage, vBond, and vSmart as the management and control elements.
- Cisco Nexus® 9K in the carrier neutral facility along with Nexus Dashboard Fabric Controller (formerly Data Center Network Manager)
- Firepower Threat Defense (FTD) is the firewall and inspection plane, and Firepower Management Center (FMC) is the management tool.
- Cisco Secure Analytics (formerly Stealthwatch) for network visibility and analytics.
- Cisco Identity Services Engine (ISE) for Terminal Access Controller Access Control System (TACACS) and Policy Enforcement using Remote Authentication Dial-In User Service (RADIUS).

Along with technical requirements, the customer needed to:

- Reduce risk from implementation challenges with optimal configurations.
- Optimize resources and costs by driving a higher success rate with scheduled maintenance windows.
- Validate end-to-end traffic flow during failure and non-failure scenarios.
- Have reliable infrastructure from a performance and scalability standpoint.
- Add additional features with minimal impact on the production environment.
- Achieve savings by outsourcing the validation.
- Leverage automation to expedite the execution of test cases.

CX Team engaged Cisco SVS to meet the above requirements.

Cisco Solution Validation Service provided test lifecycle support services, including validated designs refinement, configuration optimization, performance, scalability verification, high availability and capacity testing, software validation, deployment assurance, lifecycle management product replacement, and migration validation.

The SVS Engagement Process was broken into five phases:

Phase 1: Concept

In this phase, the customer worked with SVS to initiate an engagement request and establish a realistic scope. SVS gathered requirements, measurable success criteria, the end goal of the certification, deployment dates, configurations, and more.

Phases II and III: Engagement Request and Pipeline

In this phase, a priority was associated with the engagement request and added to the SVS engagement pipeline.

Phase IV: SVS Engagement

In this phase, confirmation that the initial prerequisites have stayed the same is crucial. If requirements have changed, re-scoping might be required. Customer and SVS established a realistic scope and execution priority for this engagement that accounted for customer milestones. SVS developed the Joint Technical Plan of Record (JTPoR) and Detailed Test Plan (DTP) to execute the scope of work, focusing on the most impactful test areas while aligning to any critical deployment milestones.

The below table lists the phases specific to the SVS Engagement Validation Process.

Table 1. SVS Engagement - Validation Process

Phase	Output	Description
Planning	Joint Technical Plan of Record (JTPOR)	▪ Conducted kick-off meeting ▪ Documented test requirements such as – Hardware and software – Network topology – Technologies and features – Traffic flows – Performance – Scale – Deployment schedule – Concerns or risks ▪ Prioritize test requirements
Test Bed	Topology	▪ Built lab topology based on certification requirements

Phase	Output	Description
Test Plan Development	Detailed Test Plan (DTP)	▪ Documented test plan to include – Test cases, data, metric – Description of test case – Devices under test – Setup details – Test procedure – Pass/Fail criteria ▪ Prepared lab topology ▪ Determined test schedule ▪ Identified risks, mitigations, and workarounds
Test Plan Schedule	Test Schedule	▪ Determined the test execution schedule ▪ Adjusted schedule based on – Change requests – Defects – Other issues

Phase	Output	Description
Testing Validation	Validated Data Configuration Files Interim Results Reports Weekly Status Reports	▪ Executed test validation - Manual - Automated (CAIT*) ▪ Customers participated in testing both remotely and onsite ▪ Interim results were provided and reviewed on an agreed-upon schedule
Results Analysis and Review	End of Test Results (EOTR)	▪ Compiled, analyzed, and reviewed results with customer

*CAIT: Continuous Automation and Integration Testing is a Cisco Service that transforms manual test cases into automated ones. The service delivers a proven validation framework, automation tools, and consulting support.

The service offers:

CX Test Automation (CXTA):

- Leverages test automation libraries on customer premises.

CX Test Automation Manager (CXTM):

- An all-inclusive, feature-rich user interface for test management.
- Provides user access to all test cases.
- Leverages open source ROBOT framework.
- Stores all execution results internally for report generation.
- Integrates into Continuous Integration/Continuous Delivery (CI/CD) and NetDevOps.

In this specific customer scenario, the Cisco lab hosted all hardware and software components, and test cases were automated using CXTM.

Phase V: Project Closure

The test bed configurations and artifacts, such as End of Test Results (EoTR), were archived in this phase.

The Cisco SVS Team validated the design with identical hardware and customer-specific software configuration in a controlled lab environment. Configurations were also tested for scalability using a traffic generator with industry-standard Internet MIX (IIMIX) and customer-specific traffic types using packets of varied sizes. SVS thoroughly tested the availability of the infrastructure during failure scenarios, along with the convergence time to meet the application demands.

Cisco SVS experts worked closely with the customer technical team at every step to successfully validate and implement the solution. The customer could access the lab setup using remote access Virtual Private Network (VPN) to review and provide feedback during the engagement's lifecycle.

While many site types and controllers were lab validated, for conciseness, only a subset of the site types and data center fabric are listed below.

Please note that SVS configured all the devices under test with customer-specific hardware and software configurations.

High-Level Campus Site Types and Data Center Topology

Campus - Site Type 1

Site Type 1 is a simple two-tier collapsed core design with wired and wireless access. This site type is considered non-critical and has no redundancy except the Wide Area Networks (WAN) transport circuits.

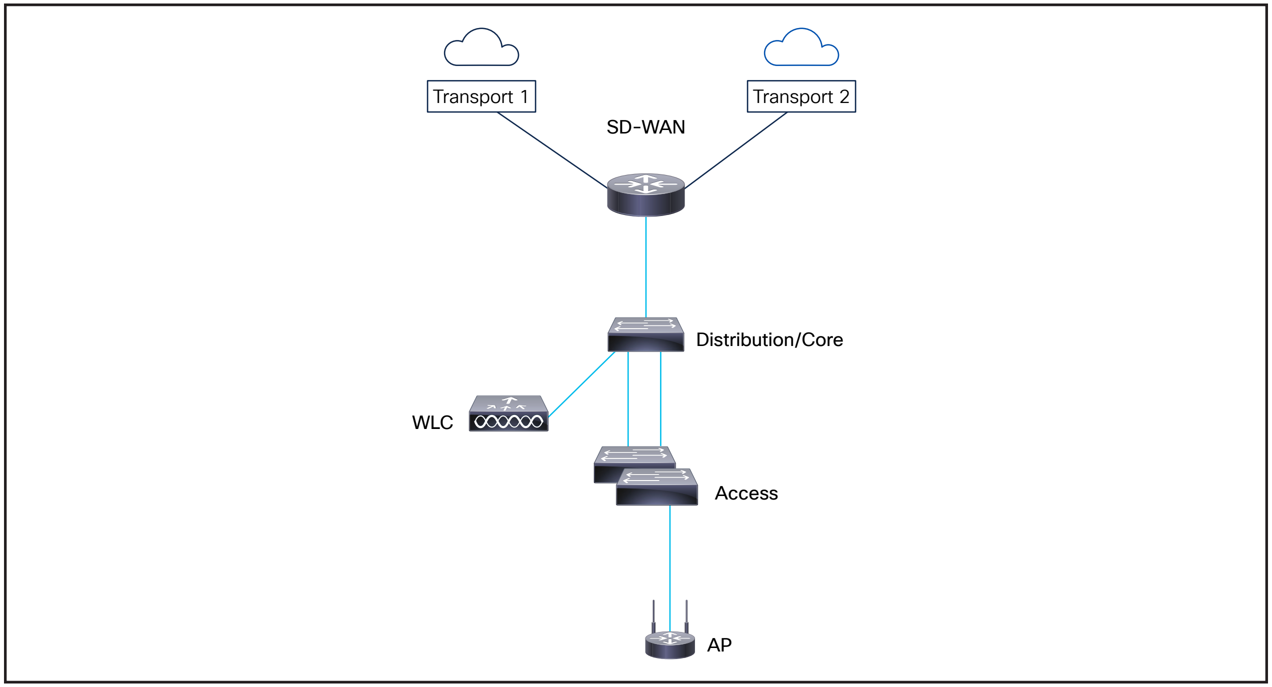


Figure 2. Campus Site Type 1

Table 2. Function and Hardware for Site Type 1

Function	Hardware
Wide Area Network	C8200
Distribution/Core Switch	Catalyst 9300 Non-PoE
Access Switch	Catalyst 9300 PoE
Wireless Controller	WLC 9800-L
Access Points	C9136

Campus - Site Type 2

Site Type 2 is a two-tier, highly available design with wired, wireless, and server access. This site type is considered critical and does have redundancy at all the layers.

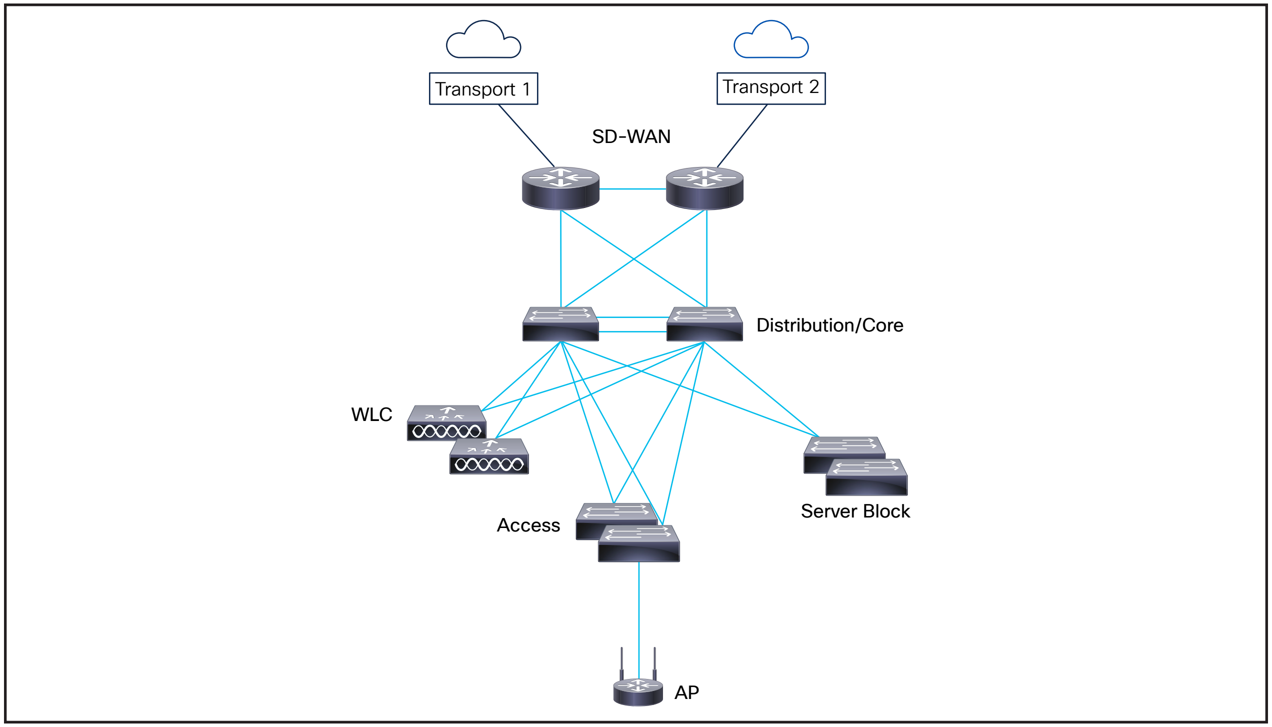


Figure 3. Campus Site Type 2

Table 3. Function and Hardware for Site Type 2

Function	Hardware
Wide Area Network	C8300
Distribution/Core Switch	Catalyst 9600
Access Switch	Catalyst 9300 PoE
Wireless Controller	WLC 9800
Access Points	C9136

Campus - Site Type 3

Site Type 3 is a three-tier, highly available design with wired, wireless, and server access. This site type is considered critical and does have redundancy at all the layers.

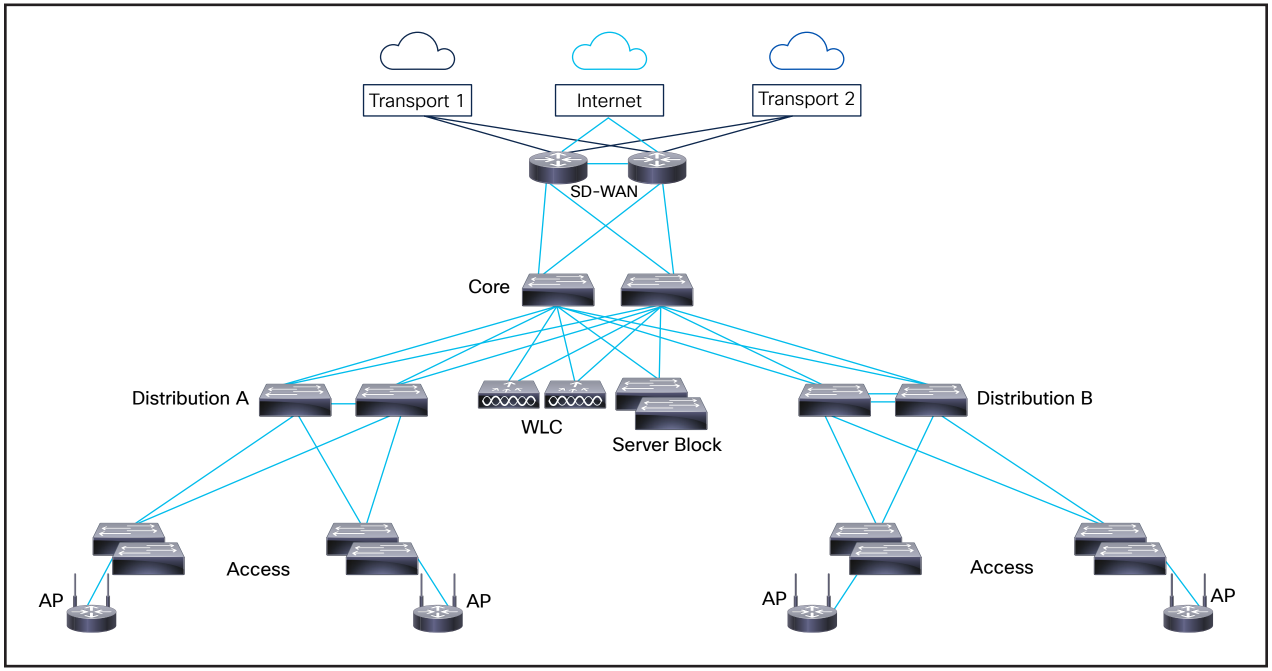


Figure 4. Campus Site Type 3

Table 4. Function and Hardware for Site Type 3

Function	Hardware
Wide Area Network	C8300
Distribution/Core Switch	Catalyst 9600
Access Switch	Catalyst 9300 PoE
Wireless Controller	WLC 9800
Access Points	C9136

Carrier Neutral Facility

The Carrier Neutral Facility is a highly available and scalable design based on Spine-Leaf Architecture.

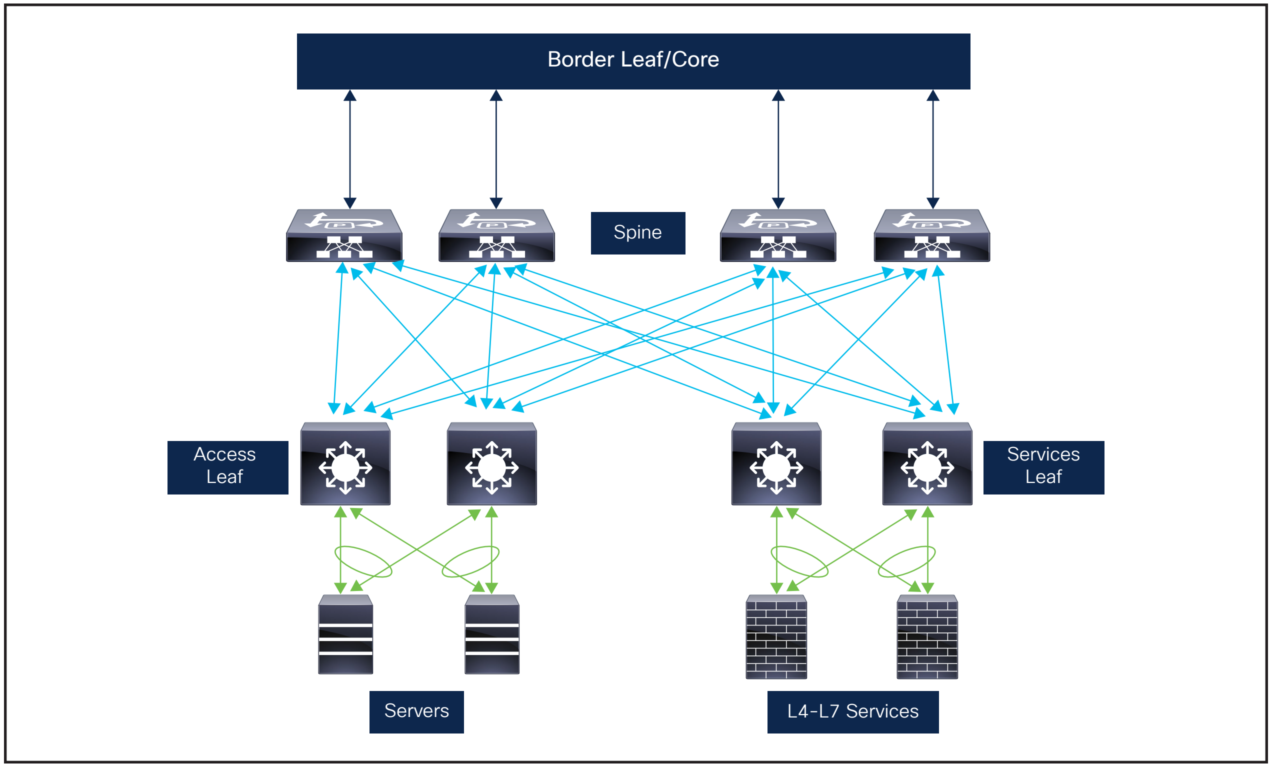


Figure 5. Carrier Neutral Facility VxLAN Fabric

Table 5. Function and Hardware for Site VxLAN Fabric

Function	Hardware
Spine	Nexus 9500
Leaf	Nexus 9300
Firewall	FTD 9300

Test Cases

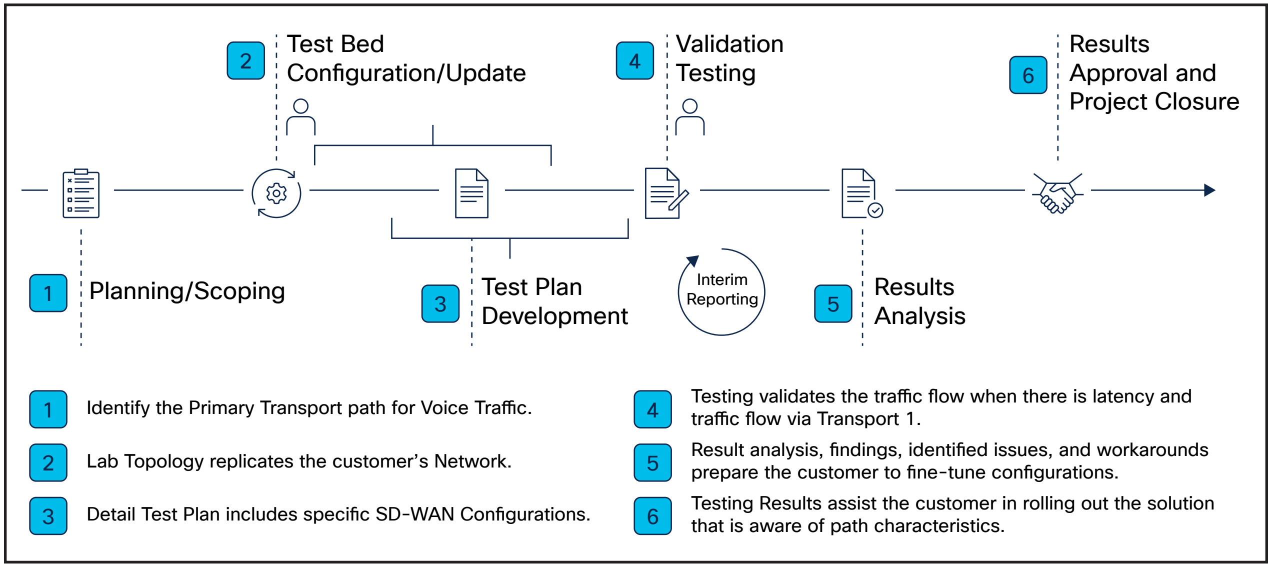
SVS validated approximately four hundred test cases across multiple products and technologies in the lab. And automation of test cases played a significant role in validating the test cases.

Table 6. Project, Technology Domain, and Number of Test Cases

Project	Technology Domain	Number of Test Cases
1	Campus Software-Defined Access and DNA Center	140
2	Software-Defined WAN, vManage, vBond, and vSmart	65
3	Data Center VxLAN Fabric and Nexus Dashboard Fabric Controller	70
4	Internet and Perimeter Network Firewalling	50
5	End Point Policy Enforcement and Identity Services Engine	90

In the interest of brevity, below are two sample test cases and the testing that SVS executed.

Sample Test Case 1: Validate Traffic Flows during Latency and Traffic Loss conditions.



1 Identify the Primary Transport path for Voice Traffic.

2 Lab Topology replicates the customer's Network.

3 Detail Test Plan includes specific SD-WAN Configurations.

4 Testing validates the traffic flow when there is latency and traffic flow via Transport 1.

5 Result analysis, findings, identified issues, and workarounds prepare the customer to fine-tune configurations.

6 Testing Results assist the customer in rolling out the solution that is aware of path characteristics.

Figure 6. Test Methodology for validating traffic rerouting during Latency on Transport 1 Path

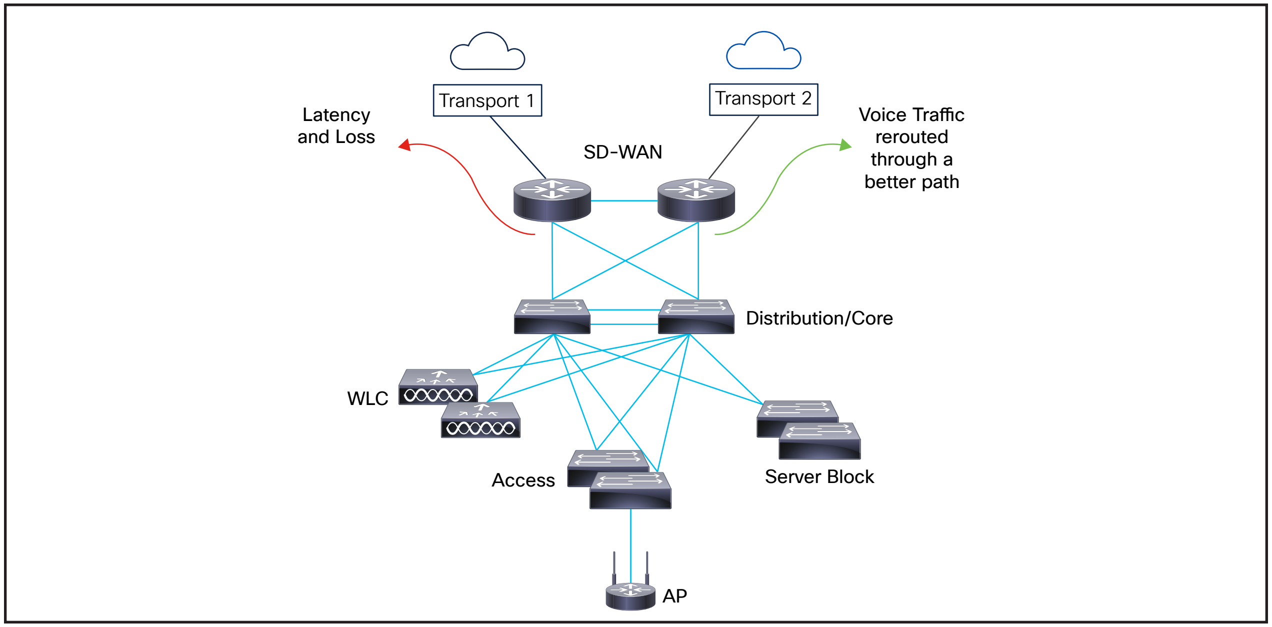
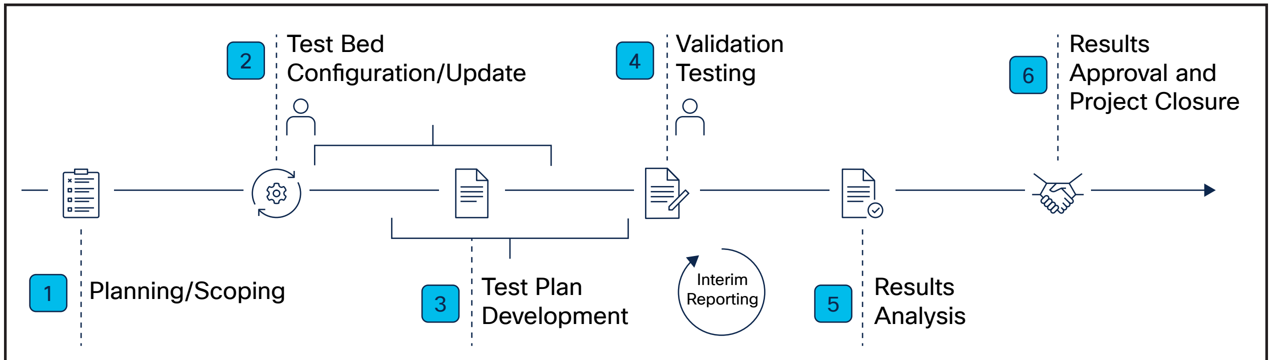


Figure 7. Voice Traffic rerouting via Transport 2 during Latency on Transport 1

Table 7. Description of the test case, set up, procedure, and pass/fail criteria

Description	Setup	Procedure	Pass/Fail Criteria
Network Performance Testing	In a normal working scenario, voice traffic will prefer transport 1 over transport 2	▪ Generate voice traffic streams using a traffic generator ▪ Verify the primary and backup paths. ▪ Introduce packet loss and delay on transport 1 leveraging traffic generators ▪ Voice traffic experiences inferior performance across transport 1 ▪ Primary (preferred) path Service Level Agreement (SLA) not met ▪ Reroute voice traffic across the alternate path, which meets the SLA requirements	▪ Voice traffic reroutes across transport 2 ▪ Routing converges on time ▪ The convergence times for the streams should be per design.

Sample Negative Test Case 2: Validate Traffic Flows during a Spine Node Failure.



1 Planning/Scoping

2 Test Bed Configuration/Update

3 Test Plan Development

Interim Reporting

4 Validation Testing

5 Results Analysis

6 Results Approval and Project Closure

1 Identify the Spine Node in the Spine failure scenario.

2 Lab Topology replicates the customer's Network.

3 Detail Test Plan includes specific Spine/Leaf VxLAN Configurations.

4 Testing validates the traffic flow when the Spine is down.

5 Result analysis, findings, identified issues, and workarounds prepare the customer to fine-tune configurations.

6 Testing Results assist the customer in rolling out the highly available solution.

Figure 8. Test Methodology for Data Center Spine Node Failure

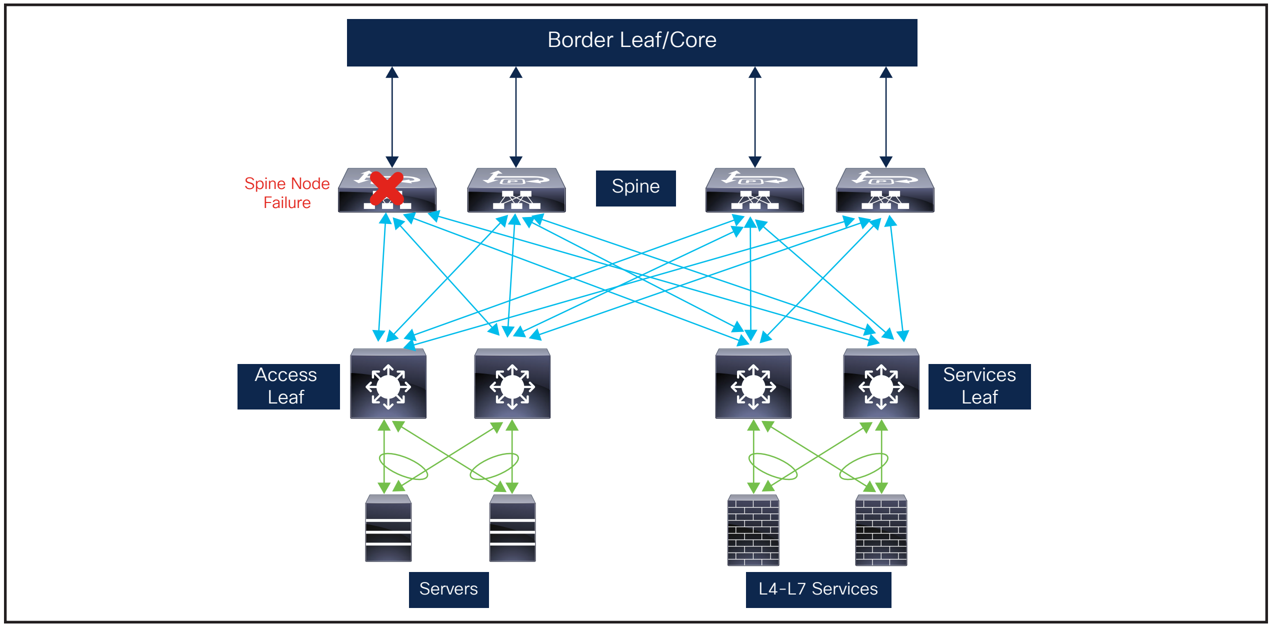


Figure 9. Data Center Spine Node Failure

Table 8: Description of the test case, setup, procedure, and pass/fail criteria for spine node failure

Description	Setup	Procedure	Pass/Fail Criteria
Spine node failure in VxLAN fabric	Spine and leaf nodes with VxLAN	▪ Clear all counters and logs on all devices. ▪ Verify the status of all links between the spine and leaf ▪ Generate traffic from the servers to a destination outside of the VxLAN Fabric ▪ Turn off power to one of the Spine nodes ▪ Measure the convergence time. ▪ Restore the failed spine and measure the convergence on recovery	▪ There should not be any unexpected dead streams ▪ Routing should converge on time ▪ The convergence times for the streams should be per design ▪ Once the node recovers, all neighbor adjacencies should be re-established

Customer Outcome

Based on the engagement of Cisco SVS and methodically executing the four hundred test cases, the customer was able to proactively identify issues and successfully implement and transform the infrastructure as planned. Due to this lab validation, the customer increased successful maintenance windows and improved efficiency in using both technical and non-technical staff.

The customer also saved 20% of OpEx and CapEx savings due to outsourcing the lab validation to Cisco SVS.

The customer also implemented Cisco SVS as a part of the Software Lifecycle Management process to certify newer software. And to further scale the testing process and meet customer time to market, Cisco SVS leveraged automation for test cases to validate the features and software versions before implementation. The automated testing led to an approximately 50% reduction in time for executing the test cases.

Acronyms

Acronym	Definition
9K	9000
AP	Access Point
CNF	Carrier Neutral Facility
CX	Customer Experience
DTP	Detailed Test Plan
EOTR	End of Test Results
FMC	Firepower Management Center
FTD	Firepower Threat Defense
IMIX	Internet MIX
ISE	Identity Services Engine
L4	Layer 4
L7	Layer 7
NetDevOps	NetworkDevelopmentOperations
JTPOR	Joint Technical Plan of Record
PoE	Power Over Ethernet
RADIUS	Remote Access Dial-In User Service
SD-WAN	Software-Defined Wide Area Network

Conclusion

Lab validation is essential for a successful network transformation in the modern world. Incorporating lab validation as part of the plan, design, implementation, and change process is vital for the successful outcome of the initiative.

This proactive approach to validating the solution, software, hardware, feature, and technology in the lab minimizes the risks and delivers a successful transformation.

Lab validation testing has become increasingly crucial as it strives to prevent problems from occurring rather than simply minimizing risks after they have already happened. This fundamental approach to prevent issues before they rise is a powerful message that underscores the critical importance of lab validation testing today.

Acronym	Definition
SGT	Scalable Group Tag
SLA	Service Level Agreement
SP	Service Provider
SVS	Solution Validation Services
TACACS	Terminal Access Controller Access Control System
VPN	Virtual Private Network
VXLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network
WLC	Wireless Lan Controller