WHITE PAPER

Network Change Management Validation with Cisco Modeling Labs 2.0

Andre Stoykovich, Program Manager Converged Data Center, Connection

Cisco Partner
Gold Certified

Connection®
we solve IT®

Business Solutions	Enterprise Solutions	Public Sector Solutions
1.800.800.0014	1.800.369.1047	1.800.800.0019

www.connection.com/cisco

Executive Summary

In this document, we will review the benefits of using Cisco Modeling Labs 2.0 (CML) to perform network change validation to help reduce the possible errors during a change control migration. Today's complex network environments require the coordination and integration of many different solutions. While each individual solution may be complex in its own right, integrating these solutions can become very challenging, and in some cases, cause unwanted downtime. In an effort to reduce mistakes that can be made during these transitions, we'll want to use every tool available to discover unknowns and test our configurations. Using CML, we will re-create relevant portions of our network in an emulated virtual environment. This will allow us to fully understand the impact of the changes we plan to make, as well as to properly design a solution that will have a high degree of success. By integrating these additional steps into our change management strategy, we'll have the ability to validate our configurations by performing the migrations virtually in CML. In this virtual environment, we'll be free to spend the quality time needed to diagnose, plan, and troubleshoot our proposed changes, all without making any changes to the production environment. We will be using a customer implementation as a test case to demonstrate how Cisco Modeling Labs can help us better plan our change management strategy, discover unknowns, and ultimately validate our proposed changes.

Problem Statement

How can we more effectively plan, troubleshoot, and validate changes to the production networks, while avoiding mistakes often made during the change management process?

Background

Today's networks are constantly evolving and becoming ever more critical to the needs of the business. Whether it's a telephony system that allows employees to communicate or the VPN solutions that allow us all to share data and work remotely, when disruptions in the network happen, many interconnected services can be affected. Internet connectivity itself has long been an essential aspect of the network and is in some cases the most important. This is even more true with the addition of Internet-based management solutions. Business disruptions can have far reaching consequences, as well as high costs, when there is unplanned downtime.

Network failures can be caused by a range of events; however, most modern solutions are resilient to such failures. Most network solutions typically have high availability options integrated into their products. Manufacturers strive to keep their products healthy by discovering bugs in their software and release updates when issues are resolved. However, much of the time, network failures often occur simply because of human error.

According to a recent study sponsored by Veriflow, only 3% of respondents said that they were able to catch and correct all their mistakes before they caused an outage.[1] The overwhelming majority of respondents agreed that human error contributed to at least some form of downtime. Fortunately, we have many processes and tools in place to minimize the mistakes that can be made when preparing to make changes in the network. Typically, this involves a change management process, so that changes can be planned and reviewed to a certain degree.

However, even within this change management process, we are still vulnerable to human error. We know that mistakes can be made when analyzing configurations or creating documentation. During peer review, it's also easy to overlook minor details or not fully grasp the implications a change will make throughout the network—especially in complex network scenarios. When changes are made to the network, it is usually a manual process that can have multiple dependencies with very complex scripts, often for multiple devices. Even with the prevalence of software-defined networking, there may still be an element of manual configuration that is required to at least integrate the solution.

In addition to making sure that changes are accurate, most of these changes require a downtime window that is often limited in length and only allows enough time for configuration with a minimal amount of troubleshooting. If issues do arise during a change management window, time is critical. In a change management scenario, extending beyond your time limits may result in partially configured, or possible completely reverted, changes. In some cases, a maintenance window may not be enough time to fully understand the implications of the changes made, and customers may be forced to schedule additional downtime to resolve other issues.

Many customers face complications with networks that they have inherited and are often challenged with integrating new solutions into legacy systems—which might not follow best practices to begin with. Cisco provides many great guides and implementation plans; however, there may be variations in your production environment that make it difficult to determine the final configuration specifics. Even with extensive planning, many customers still end up in a situation where their proposed implementation plans cannot be validated until the changes occur.

Solution

Cisco Modeling Labs is a network emulation platform that can be used to emulate virtual instances of Cisco's operating systems. While there may be other third-party options for emulating network equipment, CML 2.0 is the easiest option for emulating Cisco equipment. CML comes pre-loaded with many of the images you will need to emulate some of the most common design scenarios. They include images such as IOSv, IOSvL2, NX-OS, ASA, CSR1000v, and IOS XRv/IOS XRv 9000. It's also possible to emulate or bridge third-party appliances so that we can create a more complete virtual environment. In fact, many are built into CML, including a packet generator (TRex), a WAN emulator, and several Linux-based endpoints.

Cisco also offers an Enterprise edition of CML, which includes a whole range of upgraded features, such as multi-user environments, expanded node support (up to 300), and even TAC access. However, in the cases outlined here, the Personal edition provided all of the functionality we required. Cisco Modeling Labs is supported on multiple flavors of VMware, namely VMware Workstation, Fusion Pro, Player, and ESXi. There is also a free Sandbox edition that can also be utilized via the Cisco DevNet website, but keep in mind that access to the Sandbox has a maximum reservation time of four hours.

Rather than focus on the specific aspects of the product, we want to demonstrate the power that this tool can provide for our customers. Cisco Modeling Labs allows us to re-create real-world customer scenarios in a virtual environment, which can then be used to design and plan our implementation strategies, allow us to spend additional time troubleshooting issues, and ultimately validate our change management strategy for our customers—all without impacting the production network. This has been instrumental in helping us avoid unnecessary downtime that we might have otherwise experienced during a live migration, and most importantly, allowed us to reduce the opportunities for human error to occur in the change management process. For our test case, we want to highlight how we use CML as a component of our change management strategy for our customers.

Test Case Example: Change Management Tasks

- Customer is tasked with migrating from a legacy Catalyst 6509 in their network core to a new Catalyst 9500.
- Customer is tasked with cleaning up an existing ASA configuration, then migrating their firewall to the new core infrastructure.
- Customer is tasked with ensuring end-to-end connectivity for both the new infrastructure and temporary legacy infrastructure.
- Customer is tasked with maintaining current policy-based routing traffic flows.

Test Case Example: Emulating the Production Network

Within CML, we are able to re-create our customer's entire network infrastructure, using current configurations from each of their actual routers, switches, and the ASA firewall. We used a mixture of IOSv, IOSvL2, and even unmanaged switches to re-create the customer's routed and switched network. Even though there may be different Cisco hardware platforms throughout the customer's production network, we were able to re-create the relevant portions of internal infrastructure using generic IOSv and IOSvL2 images.

In the place of WAN connections such as MPLS or Metro Ethernet, we can use the built-in WAN emulator or even an unmanaged switch to provide connectivity between each of the remote sites. This allows us to create routing adjacencies and test connectivity from our remote sites.

The ASAv in CML should also accept a direct copy of the production device configuration. In our customer scenario, we'll want to connect this to an unmanaged switch upstream and IOSvL2 for our switches in the DMZ and Core switch infrastructure. From a command standpoint, there may be minor differences in the virtual device's interface type and slot numbers; however, the majority of the IOS-based router or switch config can typically be copied directly to each virtual device. We'll especially want to focus on establishing routing adjacencies and L2 connections to ensure that our virtual network has a routing table and access layer consistent with the production environment.

CML also gives you the ability to emulate host devices directly within the software. Here we can run Linux-based clients like Ubutu and Alpine, which are already included in CML. If required, we can import third-party images that are in QCOW2 format. It is even possible to emulate an actual Windows endpoint within CML, but in most cases using a simple Linux Desktop endpoint will provide you most of the troubleshooting tools you will need. Having these clients is useful when testing more than just basic routing/switching connectivity. Being able to emulate clients within this virtual environment allows us to better plan our change management strategy, because we can see how our endpoints react to changes in the network as well.

To help save memory and CPU resources used by CML, we can also connect our virtual lab environment to other VMs on the VMware host system using an external connector bridge. This way, we can integrate resource-intensive third-party products that might hinder the performance of CML, yet still re-create the completeness of the network.

Test Case Example: Design, Plan, Troubleshoot, and Validate Change Management Configurations

In our Customer Lab, we used CML to determine how each new device will be specifically connected in the network, and what might occur if we used alternative designs. Customer networks can become very complex over time. In some situations, a temporary network design may be necessary as a steppingstone on the way to our ultimate design goal. In our Customer Lab, we found several design inconsistencies with the ASA and DMZ switching infrastructure that needed to be addressed before our proposed changes would work. These connectivity issues may not otherwise have been found until the validation phase of our network cutover.

Once our design of choice has been determined, we can further plan our change management strategy by performing simulated cutovers or migrations within CML. This gives us the ability to run multiple cutover scenarios to determine the best path forward and which resources we might need on hand for the migration. In many situations, customers may be required to make configuration changes remotely. In this scenario, it is especially important to plan the order in which you make changes. In our Customer Lab, we were able to test our migration plan from the perspective of a remote VPN host making changes to the infrastructure during the migration window. We were then able to identify several devices that might lose connectivity during our mock migration. This allowed us to review every affected configuration and avoid the connectivity loss that might have occurred. In the end, we were able to put our implementation plan to the test and avoid additional downtime or possible rollbacks since we were able to see these connectivity issues play out during our mock migrations.

As we know, migration windows are typically limited in time and scope. If we do run into issues during an actual migration, we often do not have enough time to properly diagnose an issue before a rollback is required. Since critical systems are given priority in these scenarios, this might lead to incomplete or inconsistent configurations elsewhere in the network. Often, issues may fall under the radar during a migration and aren't discovered until after the maintenance window has ended. By performing mock migrations in CML, we have additional time to review the end-to-end connectivity that we might not be possible during a live migration. During our mock migration, we found that while PBR was properly routing in most instances, there were several traffic flows that were taking an undesirable route. During a live migration, this might have gone unnoticed since basic connectivity test would have passed. In fact, it may not have been discovered until well after the maintenance window was complete. Having this extra troubleshooting time in our CML lab was vital in avoiding additional changes that might have been necessary after our initial cutover. Within this virtual environment, we were able to drill down into the specifics of the configuration and take the extra time needed to fully understand our traffic flows after performing a mock migration.

Conclusion

With Cisco Modeling Labs 2.0, we were able to re-create our customer's production network in a virtual environment and to perform simulated migrations. This allowed us to further understand the customer's end-to-end infrastructure and discover sub-optimal behavior post-migration. We were then able to improve our design and implementation strategy. Since we performed our configuration changes several times in CML, we were able to successfully accomplish the customer's tasks with confidence and avoid many of the pitfalls that were discovered in the virtual environment.

In the context of making changes to a production environment, typically the biggest risk to unnecessary downtime is due to a breakdown in the change management strategy caused by human error. Ultimately, Cisco Modeling Labs strengthens our change management process by allowing us to validate our design, implementation plan, and proposed configurations changes, all without impacting the customer's production environment.

While we may not be able to remove all aspects of human error from our network change management strategy, CML provides us an additional tool and experience to help us reduce—and often eliminate—unnecessary downtime for our customers.

[1] Top Reasons for Network Downtime https://www.networkworld.com/article/3142838/top-reasons-for-network-downtime.html.

References

IT Challenge: Pace of Change with Infrastructure https://www.informationweek.com/strategic-cio/it-strategy/it-challenge-pace-of-change-with-infrastructure/a/d-id/1336124

Calculating the Cost of Downtime https://www.atlassian.com/incident-management/kpis/cost-of-downtime

Cisco Modeling Labs https://developer.cisco.com/docs/modeling-labs/

Cisco Modeling Labs Breakout Tool https://www.cisco.com/c/en/us/td/docs/cloud_services/cisco_modeling_labs/v200/configuration/guide/b_cml_user_guide_2-0/m_breakout_tool.html

Network Change Management Best Practices https://www.networkcomputing.com/networking/network-change-management-best-practices

A Trusted Partner

As a leading National Technology Solutions Provider, we've been trusted for more than 35 years to connect people with technology that enhances growth, elevates productivity, and empowers innovation. Connection stands ready to deliver, install, and maintain technology nationwide by leveraging our internal professional services expertise and top-tier vendor partnerships.

Business Solutions	Enterprise Solutions	Public Sector Solutions
1.800.800.0014	1.800.369.1047	1.800.800.0019

www.connection.com/cisco