



# Standardized Switching for Architecture Readiness

Joe Blazon  
Director Solutions Operations

Craig Mock  
Consulting Engineer

## INTRODUCTION

Enterprise networking vendors have long been touting the simplicity of the solution-defined architecture. While the result provides a powerful solution with a more robust set of tools, the road to the complete stack can be long and difficult to navigate. Most IT (Information Technology) departments have limited standardization, or documented standardization throughout their network infrastructure; typically, only keeping within the same OEM manufacturer but invested across multiple models serving the same purpose. From our view this is commonly caused by mismatched technology refresh cycles, legacy devices' inability to serve multiple use cases, or just the preference of any given engineer or manager in charge of procurement at the time of purchase. Whatever the case, the un-forecasted result can be a disparate network that is difficult to manage. Recognizing the value of being hyper-focused on specific solutions within a specific family of switches and/or routers will allow day-to-day maintenance tasks to be kept to a minimum, allows for more repeatable processes, and enables teams to pivot their focus to more strategic work for their respective business. This white paper will demonstrate the thought and methodology for a technology refresh utilizing enterprise-class Cisco network switches and standardization of access layer switching.

## CUSTOMER CHALLENGES

The subject within this paper is an actual Zivaro client. They are a large organization with multiple distributed departments, 35,000-plus employees, and unique requirements across functional groups. While there is an overarching security group, most of the day to day and operations are distributed throughout multiple IT departments. Although the current design has network management de-centralized, there are individual contributors and network engineers that transfer between departments from time to time and collaboration is encouraged but not mandatory. There is a growing movement, in part advocated by our team, supporting a desired end-state of standardizing network infrastructure throughout all departments. This large organization has 10-12 different models of switches with many of them approaching End of Life (EOL) with Last Day of Support (LDoS) in the next one-to-five years. When doing analysis to assist in determining replacement models, two primary requirements have become known:

1. The anticipated lifespan of the equipment needed to be closer to 10-12 years or more in length instead of the 5-7 years they were currently experiencing with many of their entry-level access switches.

2. There needed to be standardization between models for cyber security purposes and incidents of Product Security Incident Response Team (PSIRT) notifications, and proactively knowing if devices required patching. When the vendor previously sent a notice on a vulnerability it would take a significant amount of time to analyze the impact on the organization and individual departments.

With these two primary requirements identified, the methodology for selecting switching hardware for the access layer could be determined, along with some other fundamental assumptions on reducing complexity, increasing Power of Ethernet capabilities, and automation.

## BACKGROUND

The large organization we refer to in this whitepaper had various models of access layer switching including Cisco Catalyst 2960S, 2960X, 3750, and 3850's in their production environment. Many of these switches have gone or are going End-of-Life sometime in the next five years. During an initial lifecycle review and budget planning session, we identified each department and revealed the extent of this switch variety. Unfortunately, the traditional Cisco planning tool was not constructed to evaluate environmental factors and thus cannot be solely relied on to identify recommended replacements (in fact that is the purpose and value of a partner like Zivaro). Many times, the Cisco tool recommendation included a model for a switch which was only a year or two newer than the one we were replacing and had already announced End-of-Support itself, which posed a challenge when attempting to standardize on a specific model. I want to clarify that the Cisco configuration support tool for partners is an excellent resource, but its outputs still need to be doublechecked as part of a fool-proof design deliverable.

By taking more of a consultative approach and focusing our attention on how the organization should standardize, we found there to be a significant level of effort to replace switches on the scale necessary. Part of the process was to review any documentation throughout the organization that provided guidance on selecting access layer switches. To remind the reader again, this org. has 35K-plus employees distributed across roughly 15 distinct sub-organizations with some shared services but many others under autonomous direction. It was found that little to no documentation existed on methodology for what switch requirements were needed (why, where etc), cost standards required, recurring annual support costs, or advanced licensing requirements such as DNA (Digital Network Architecture). An early and critical step in our process was to help the client with defining the requirements and long-term cost of ownership which then allowed for initial mapping and a standardization roadmap of switch models. In this step we also identify high-level trade-offs and benefits from one model vs. another. Enough cannot be said about this phase because, like any technology project if the requirements are not gathered in enough detail, then eventually someone or some department is going to have shortcomings with the chosen platform.

---

## THE SOLUTION

The solution we proposed included standardizing the various switch models used at the access layer into four models of access layer switches. The organization had no requirement around a modular switch technology (the ability to upgrade the module to provide higher speed interfaces in the future such as moving from 1Gb to 10Gb for growth), so the fixed format switches were proposed as the logical choice and proved to be the most cost-effective solution. An additional requirement was power-over-ethernet (POE) on every switch due to the prevalence of Internet of Things (IOT) “smart” devices including temperature controls and monitors, water leak detection, door access controls, and POE Video surveillance cameras. Long-term use and planning for networks must include support for POE, or POE+ on all ports even in many data center access layer areas. The next thing we considered was the uplink speed: 1Gb or 10Gb fiber or copper. Once we determined the uplink requirements, we decided on the four models for standardization. All four models run the same firmware and have the same security profile in addition to having similar overall characteristics. The Cisco 9200L fixed format model were the most sensible fit for most of the switches in the access layer. The first two Cisco C9200L-24P and C9200L-48P provide POE and POE+ capabilities for both models. The other two standard switches, Cisco C9300L-24P-4X and C9300L-48P-4X, provide 10G uplinks and offer redundant power supply options and stack power for more critical functionality within the infrastructure.

As the client contemplated a longer-term roadmap to network programmability and automation, the process of evaluation also included important analysis around the DNA software subscriptions that accompany every switch. The features and benefits increase exponentially from the entry-level subscription (DNA Essentials) to the fully loaded subscription (DNA Premier). A few of the key benefits evaluated included the following software subscription capabilities:

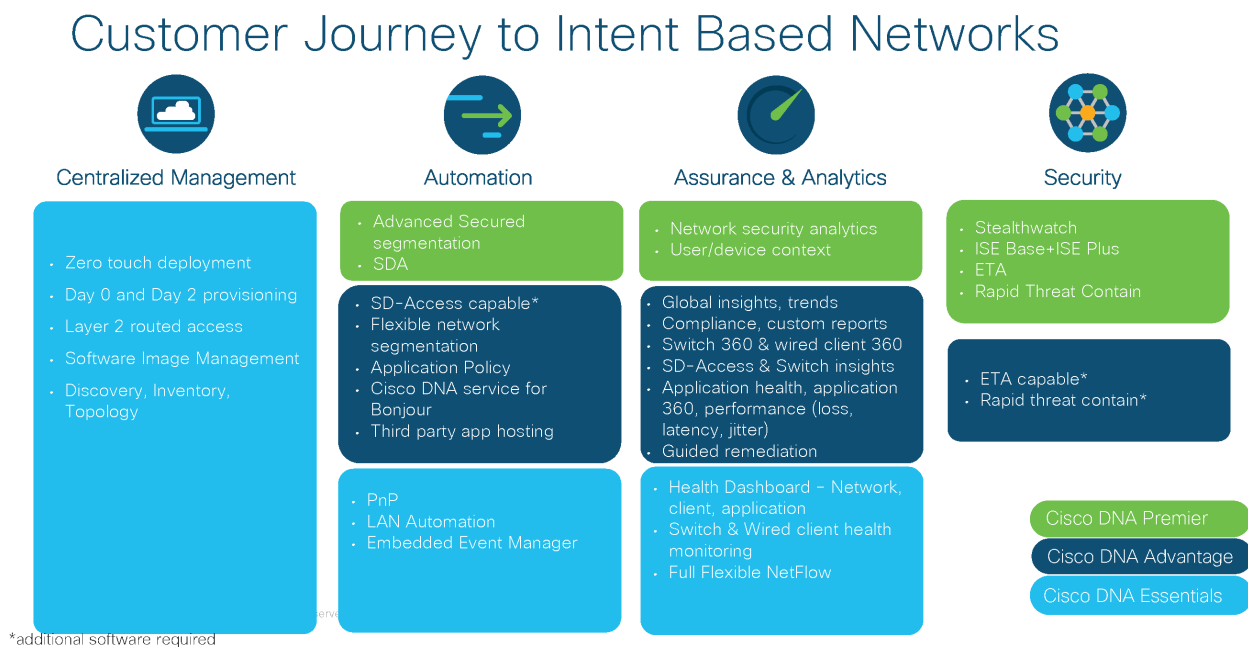
- Cisco Identity Services Engine (ISE): Leveraging ISE for policy creation allows for a standardized security profile throughout all the switch fabric, minimizing the time to implement and maintaining a base security posture throughout the environment by pushing said policy with the assistance of DNA Assurance.
- Cisco DNA Center Automation: Fully utilize resources and user experiences, Cisco DNA integration with Cisco 9200 switches enable operation simplification and automation and configuration of ports for allowing better wireless and IoT (Internet of Things) support.
- Enablement and adoption of intent-based networking across the entire switch fabric to include wired and wireless for simpler network management by implementing application-aware policies for users and devices and automating repetitive tasks.
- Assurance and Analytics: Extending visibility, decision support and analysis capabilities in the wireless networking environment.

In the consulting process we needed to unearth answers to crucial factors which could affect long-term success for the IT department. What is the state of readiness of the organization for advanced features? Are they a DevOps shop already and open to further automation capability? Do

---

the network administrators have existing skills in ISE or automation (i.e., programming), or do those skills need to be acquired? Are the lines-of-business applications slowed down with existing architecture and operations? In the case of this customer, they are implementing ISE for particular use cases but are not currently prepared from a resource perspective to contemplate a lot of automation. Given this timing issue related to their internal capability, we elected for shorter-term DNA Advantage subscriptions to get some of the newer software functionality out of their ISE deployment but giving them the flexibility to modify the subscriptions later at a higher level with deeper functionality as they can consume it. Another unsung benefit of the DNA subscriptions is their license portability – by simply having switches with DNA subscriptions customers can move or change underlying switches if conditions change and preserve their original software investment.

Figure 1: Below highlights the licensing requirements for customers going down the intent-based path.



A final small yet critical benefit of the proposed solution was the equipment lifespan and anticipated support periods for the new equipment. The Cisco 9200 and 9300 have an estimated 12+ year lifespan. The lifespan of the devices we considered here is different than Mean Time Between Failure (MTBF), which is a calculation based on the components in the system. The lifespan, in this case, refers to the time from the first sale to the last day-of-support date. This is important as most network operators know the longevity of Cisco equipment, and for current best practices and compliance reasons, the equipment must be always supportable by the manufacturer including both hardware and software patching for vulnerabilities. It is a common trap with disparate switching environments for customers to find themselves in a crisis outage only to realize an ancient switch was left in production to 'save' money.

## CAVEATS AND SWITCH SELECTIONS

With many large series of switches in the past 30 years, there have been models that have been sunset sooner than the rest of the group. As an example, an early Cisco 9300 model (the 9396TX) announced EOL May 1, 2017 which was primarily a dense 10G Copper switch. There are always reasons for the early retirement of a switch. Some of these include improvements in the manufacturing of newer models, slow sales, similar and less expensive models making the device obsolete, or a more resilient higher-end switch surpassing the model in question. No matter the reason for the caveat of some models being EOL early, when evaluating and choosing switch architecture to standardize on, pick the best one for your environment and look at a few things:

- MTBF – Mean Time Between Failure (These are usually provided in hours and):
  - Look at the Data Sheet below and search for MTBF and you will see a range of the 9300 in hours from 198,647 (22.67 years) to 395,800 (45.18 years)
  - This MTBF is an engineering calculation done on the components and entire switch so depending on how it was put together with what components will change this number. This does not tell how long the switch will be able to run in production but may give a glimpse of its reliability expectation.
- Release Date: Product release dates are important. If looking at a switch that is 11 years old to replace a switch which is EOL and was released 12 years ago, you should probably keep looking.

This client has taken some substantial and positive steps in their overall architecture planning processes which should improve their readiness for further advances. We now have a standing monthly meeting cadence where hardware, software and support lifecycle issues are consistently reviewed as part of a longer-term analysis of requirements to ensure we are collectively ahead of planning cycles. This has been close to a two-year journey marching towards better standardization. The progress has been slow at times due to the network's complexity, budget cycles, staffing and other hurdles but continues to show forward progress and maturation. This switch analysis exercise is also proving to be a critical component of an upcoming evaluation of SDWAN alternatives.

## CONCLUSION

There are many benefits of migrating from multiple types of switches to a more standardized approach, much of which were expressed in this document. While the solution discussed may not be an exact match for every environment, simplified management, lower TCO (Total Cost of Ownership), capability, and flexibility are common benefits every organization seeks when making their technology decisions. Simple, often overlooked factors such as projected lifespan, support windows, and cross-compatibility can have costly effects on performance and manageability. Leveraging the overarching Cisco switching platform and standardizing creates real opportunities to take advantage of architectural advancements and automation while simplifying management and operations for network teams. By taking a thoughtful and longer-term view of an organization's entire switching environment, more requirements are vetted, and more alignment between business needs and technology takes place. Cisco's switching portfolio with its programmability and automation

---

capabilities, along with Zivaro's advisory support offers substantial opportunity to create a more robust and sustainable switching environment with flexibility, lower TCO and advanced capabilities to take any organization into the future.

## ABOUT ZIVARO

Zivaro, Inc. provides industry-leading consulting and technology services to help clients realize measurable business value from their technology investments. Clients leverage Zivaro for a broad range of consulting, deployment, and operational support across hybrid cloud infrastructure, application development, security operations, and workforce collaboration tools. With deep roots in network infrastructure, Zivaro helps plan, build, and operate complex, multi-cloud architectures with an emphasis on security policy and control for public sector and regulated environments.

## REFERENCES

### Cisco Catalyst data sheet

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html>

### Cisco Catalyst Architecture

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-architecture-cte-en.html>

### Cisco End of Life Policy – Product Lifecycle Overview

<https://www.cisco.com/c/en/us/products/switches/eos-eol-policy.html>

### Cisco Enhanced Limited-Lifetime Warranty

<https://cs.co/ELLW>

### Cisco Licensing for Switches

<https://www.cisco.com/c/dam/en/us/products/collateral/software/one-subscription-switching/dna-licensing-switching-subscription-bdm.pdf>