Prepared for

opentext™

The Future of Your NetOps Toolset: Planning for Cisco Prime Infrastructure End of Life

March 2024 EMA White Paper

By **Shamus McGillicuddy**, Vice President of Research
Network Infrastructure and Operations

EMA™
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

This advises IT organizations on how to plan for the retirement of Cisco Prime Infrastructure, the network infrastructure vendor's longtime network management tool suite. It identifies key trends that are guiding IT tool strategy today and provides an overview of what decision-makers should look for in their next network management solution.

It's Time to Replace Cisco Prime Infrastructure

IT organizations have used Cisco Prime Infrastructure to monitor and manage Cisco-based networks for many years. That time is coming to an end, with Cisco announcing plans to retire the solution. IT leaders need to plan for a transition to a new tool. They should use this moment as an opportunity to transform network operations.

Cisco Prime End of Life is Here

Cisco Prime Infrastructure is a suite of appliance-based products that provide lifecycle management of Cisco-based enterprise networks. More specifically, IT organizations use Prime to manage Cisco routers, switches, and Wi-Fi infrastructure in campus and branch environments. It provides two core areas of functionality. First, it supports network element management tasks, such as device discovery and configuration management. Second, it offers monitoring and troubleshooting workflows for fault management and performance management.

"Prime is my primary tool, especially for monitoring access points," said a network manager with a Fortune 500 business services company. "What's most useful is being able to push code through it that initiates reboots or changes configs. In this building, every room has a Cisco 3560 switch, so I'm managing 800 of them. If I was trying to update code manually on those switches, it would take me days. With Prime, I can script it and push the change to every machine at night and just let it run. I can upgrade everything in about four hours."

Recently, Cisco formally announced end of life plans for these tools. It is no longer selling Cisco Prime Infrastructure and the cessation of all development and support of the product is on the horizon. Cisco will cease maintaining the product on September 28, 2024, meaning it will no longer release bug fixes and improvements to the tool. On September 28, 2025, Cisco will cease issuing security updates and patches for the product. On Sept. 30, 2028, it will end customer support for the product. Given these announcements, all users of Cisco Prime Infrastructure should look for a replacement solution immediately.

An Opportunity to Rethink Network Management

With its retirement of Prime, Cisco is recommending a migration path to a replacement Cisco product. While many IT decision-makers may choose to follow Cisco's recommended migration path, all network teams should do due diligence to ensure that their choice is best for their organization.

IT decision-makers should start by looking at their existing toolset. While many IT organizations use Cisco Prime, very few relied on it as their sole network management solution. The organizations usually supplemented Cisco Prime with multiple third-party tools to fill gaps in scope and functionality. Enterprise Management Associates (EMA) research traditionally finds that the typical network team uses between four and fifteen tools to monitor and manage networks. There are obvious inefficiencies in such a tool strategy.

While many IT organizations use Cisco Prime, very few relied on it as their sole network management solution.

"For its time, Prime was quite good," said a senior project manager with a large government agency. "But the moment we started using software-defined networking, we needed something more. We need more automation, more telemetry, and more visibility."

Functionality

Now is the time for network teams to consider a more unified, end-to-end approach to network management. EMA recommends that network teams look at ways to unify and integrate two key areas of functionality: configuration management and performance management. In other words, they should look for a comprehensive platform that supports network discovery, automated network provisioning, network monitoring, fault management, performance monitoring, configuration management, and compliance management. **Figure 1** provides a comprehensive overview of the capabilities an IT organization needs to find in a Cisco Prime replacement.

Figure 1. Cisco Prime Capabilities You Need to Replace

Network discovery	• Discover existing network elements • Inventory device information • Collect existing configs • Discover and map topology/dependencies
Automated network provisioning	• Design network configs and services in a single pane of glass • Automatically provision devices when they connect
Network monitoring	Collect, report, and analyze network telemetry, including: • SNMP MIBs and traps • NetFlow/IPFIX • Network-Based Application Recognition 2 (NBAR 2)
Fault management	• Alerts on events and thresholds (SNMP) • Classify alerts by severity • Acknowledge/Assign/Clear alerts
Performance monitoring	• Collect and analyze network flows (NetFlow/IPFIX) for insight into users, applications, traffic patterns, and traffic volumes
Configuration management	• Write config changes • Review and commit changes
Compliance management	• Set “golden” configs for network equipment • Audit devices against config standards • Remediate config standard violations

Multi-Vendor Support

Decision-makers should also think about scope. Cisco originally designed Prime Infrastructure to manage Cisco-based networks, with only limited support for managing third-party network infrastructure products. Given that most enterprises have multi-vendor networks, network teams should look for a management solution that can support multiple network infrastructure vendors without any variation in visibility and control from vendor to vendor.

"We're looking for a config management tool that is multi-vendor," said a network engineer with a government contractor. "We have Palo Alto Networks firewalls and Riverbed WAN optimization, and third-party support of config management in Prime is not well done."

The Stakes: NetOps Must Improve Tool Strategy

EMA research revealed that network operations teams are increasingly struggling to maintain their networks. Over the last six years, EMA observed a decline in the number of enterprise network operations teams that were fully successful in managing their networks, from 49% in 2016 to 27% in 2022.[1]

The tools that a network team uses can determine its destiny. EMA research identified several major issues that organizations have with their network management tools. First, 26% said that limitations in tool scope are causing significant pain.[2] They cannot manage everything they need to manage with a single tool. This is particularly an issue in multi-vendor networks, in which a tool like Cisco Prime Infrastructure will have little support for non-Cisco equipment. Some tools also cover only a portion of the network (e.g., campus networking and Wi-Fi, but not the data center network or the cloud).

Alarm noise is another problem. Twenty-one percent said noise is a top challenge for their network management toolsets. Also, the average IT organization believes that 53% of the alerts coming out of their network monitoring tools are false alarms.[3] Thus, they need tools that offer effective alert management features that reduce false alarms and consolidate events into larger incidents.

More than 21% of network teams told EMA that their tools fail to provide them with insights. Instead, their tools present data in dashboards and reports with limited context and analysis. Network engineers must work out in their heads what the data means. In conversations with network operations professionals, EMA has heard time and again that network management tools must do a better job of turning data into actionable insights.

"We're looking for a config management tool that is multi-vendor," said a network engineer with a government contractor.

26% said that limitations in tool scope are causing significant pain. They cannot manage everything they need to manage with a single tool.

[1] EMA, "Network Management Megatrends 2022," April 2022.
[2] EMA, "Network Observability: Delivering Actionable Insights to Network Operations," October 2022.
[3] Ibid.

Finally, 21% of network teams struggle with data quality in their tools. Often, their tools can't collect data reliably due to tool architecture issues or network complexity and scale. The tools also struggle to store network data effectively because of issues with backend databases. In fact, 87% of network teams told EMA that the volume and variety of data that they collect with their tools increased in recent years, challenging data quality.[4] These are the top data issues that network teams have with their tools today:

1. Data conflicts between tools (46%)
2. Data collection issues (45%)
3. Data storage limits (44%)
4. Data silos within individual tools (36%)

Overall, visibility is a major issue for network teams today. Only 8.5% told EMA that they can easily get a global view of their entire network with their existing toolsets, and only 24% are fully satisfied with how their tools support network troubleshooting.[5] As a result, network teams are doing a lot of fire-fighting. End users detect and report 31% of all network problems before the network operations team is aware of them.[6]

Network configuration management and compliance are ongoing tool issues for network teams. In the average network, manual configuration errors cause 27% of all network problems, and that percentage climbs higher if the network team is using a larger number of tools. Tool consolidation is an imperative.

Only 8.5% told EMA that they can easily get a global view of their entire network with their existing toolsets.

What to Look for in Your Next Tool

Network teams should recognize the end of life stage of Cisco Prime Infrastructure as an opportunity to optimize their toolsets. Over the years, EMA has surveyed thousands of IT organizations and interviewed hundreds of network operations experts on this subject to identify best practices. These are our recommendations.

[4] EMA, "Network Observability: Delivering Actionable Insights to Network Operations," October 2022
[5] Ibid.
[6] EMA, "Network Management Megatrends 2022," April 2022.

Adopt a Unified Platform

One consistent theme in EMA's research from year to year is that network teams do better when they adopt fully integrated, multifunction platforms rather than narrowly focused best-of-breed tools or loosely integrated tool suites. Yet, many network teams continue to have very large toolsets, which leads to trouble. For example, network teams who use one to three tools to monitor and manage their network report that configuration errors only 23% of network problems, while teams that use 21 or more tools report that such errors cause 34% of problems.[7]

Network teams do better when they adopt fully integrated, multifunction platforms rather than narrowly focused best-of-breed tools.

"We would prefer to use just one tool and deal with just one vendor when we have problems, but I don't see that happening. We can't find a company that can do that kind of consolidation for us," said a network engineer with a government contractor.

IT decision-makers must recognize this challenge and push their tool procurement teams to adopted unified solutions. One huge opportunity is the unification of network performance management and configuration management. When workflows are unified and reporting and alerting are integrated across these two domains, network teams can streamline operations. For instance, such a platform offers a time series dashboard that maps configuration changes to fault and performance indicators, which quickly pinpoints how a network change impacted network state.

Establish a Network Data Lake

Network data is extremely valuable, but it's also becoming unwieldy. Network teams are collecting larger volumes of data and more types of data to manage and analyze their networks. Thus, the tools that collect this data must have an architecture that can handle data-related challenges. Tool procurement teams should seek tools with backend databases that facilitate innovation and integration.

EMA research found that 83% of network teams are interested in streaming data from their tools to a network data lake.[8] Many organizations stream data from their tools to a standalone data lake, but others prefer a network management tool that has a modern data lake platform natively integrated into it. Such a platform can consume data from other tools and establish a source of truth for the network.

83% of network teams are interested in streaming data from their tools to a network data lake.

[7] EMA, "Network Management Megatrends 2022," April 2022.
[8] EMA, "Network Observability: Delivering Actionable Insights to Network Operations," October 2022.

The following are top use cases for a network data lake[9]:

1. Collaboration (58%) – A data lake empowers the network team to share data with other teams, like DevOps and cybersecurity.
2. Data retention (55%) – Data lakes are highly scalable, allowing network teams to maintain their data retention requirements even as the volume of data collected from the network explodes.
3. Data correlation across tool siloes (48%) – Network teams continue to struggle with tool consolidation. A data lake allows them to pull data from disparate tools and consolidate insights centrally in a multifunction platform.
4. Audits (43%) – Audits and compliance reporting are time-consuming tasks for network teams. A powerful data lake makes it easier to fulfill these requirements.

Prioritize These Features and Capabilities

Network teams should think about the capabilities of their next network management solution at two levels, first from a high-level platform perspective, then from a feature and functionality perspective.

Platform Requirements

At the platform layer, network teams tell EMA that four characteristics are most essential.[10] First, they need their solution to **integrate with other IT management systems**, both network management tools and tools in other silos, such as cybersecurity, DevOps, data center operations, and IT service management. Given this criticality, procurement teams should interrogate prospective vendors about their application programming interfaces (APIs), documentation of those APIs, and the software development kits available for those APIs.

Next, network teams are emphasizing **ease of use**. The tool should have rich functionality that allows highly skilled engineers to dive into it as power users. The tool should also have workflows that are designed for lower-skilled admins, allowing them to deliver more value to the organization by taking more tasks off the shoulders of power users. “Our veteran employees are very familiar with Prime, and they think it’s very easy to use and intuitive. But its time is up. The next tool can’t be complicated,” said a senior project manager with a large government agency.

[9] EMA, “Network Observability: Delivering Actionable Insights to Network Operations,” October 2022.
[10] EMA, “Network Management Megatrends 2022,” April 2022.

Low maintenance and support costs are also a major focus. Many tool vendors have shifted from perpetual licenses to subscriptions. This shift means that annual budget outlays for tools are going up. Network teams need to control those costs while also maximizing the level of support they get from their vendors.

Finally, network teams are looking for tools that deliver a **rapid return on investment**. This means that the time to value for a tool should be quick. IT organizations want to install the tool and start managing the network with it quickly.

Feature Requirements

EMA research identified six features that are most essential in network management solutions.[11] Network managers listed **data visualization** as their highest priority. They want innovative approaches to translating data into actionable insights. Tools should do more than just make network data accessible for analysis. They should present that data in a variety of dashboards, reports, and maps that help personnel derive meaning from it.

Traffic analysis is another major requirement. Network teams need more than device statistics and events to understand what's happening. They need to see how traffic is flowing across the network, at what volumes, and for what purpose. Network tools that can analyze flow records or even packets can deliver tremendous value.

Change detection and validation are also essential. Alerts on bad network changes can help network teams correlate those changes to network problems. On the flipside, validation of changes helps network teams verify that good changes to the network were actually implemented. Too many network teams push changes to a network and rely on incoming trouble tickets to tell them whether the change was successful. A proactive validation of a change eliminates errors and improves documentation and auditability.

Alerts on bad network changes can help network teams correlate those changes to network problems.

Alert management is another top feature requirement. Network monitoring tools produce a lot of noise, and this paper established that most are false alarms. Network teams need features that allow them to tune alerts to thresholds that are specific to their business. They also want functionalities that allow them to correlate events so that one device failure generates one alert, rather than dozens or hundreds of alerts from systems that are affected by that failure.

[11] EMA, "Network Observability: Delivering Actionable Insights to Network Operations," October 2022.

Network discovery and dependency mapping is a foundational feature. Network teams often have limited visibility into what's on their network. Strong discovery features can light up that darkness. More importantly, it speeds up the time it takes to start monitoring everything in an intelligent way. Tools must be able to discover network devices and map dependencies between them. Some network teams will want even deeper discovery capabilities, being able to extract configuration files, for instance, and codifying that configuration information into a database.

Finally, **data searchability** is important. Many tools summarize network data and present that into their dashboards and reports. Then, they discard the raw data. Network teams that are doing deep analysis for troubleshooting and capacity planning will want that raw data. More importantly, they want to find it without too much effort. So, an advanced search function that allow them to search by multiple variables will deliver powerful benefits.

"I like the way Prime lets you separate and filter for devices in the dashboard, such as switches, models of switches, and controllers," said a network manager with a Fortune 500 business services company. " I want to be able to find specific devices. If someone came along with a product that gave you that same functionality and granularity to drill down to subgroups of hardware, I would look at that product."

Conclusion

The clock is ticking with Cisco Prime Infrastructure. If your network team uses it in any way, they must start planning for a replacement. While Prime excelled at managing Cisco-based networks, it was never truly a multi-vendor network management platform. That is why so many network teams that used it also have several other tools that they use daily.

Now is the time to rethink their entire approach to tooling. If a network team is going to replace Cisco Prime, it should also look at how it can improve the rest of its tool stack. EMA recommends that network teams embrace multi-vendor network management solutions that unify functionality across network performance management and network change and configuration management. Some network management tool vendors, such as OpenText, excel in providing such a platform that is scalable and rich in features. This paper provides a roadmap for how to select the right tool for you.

The clock is ticking with Cisco Prime Infrastructure. If your network team uses it in any way, they must start planning for a replacement.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com**. You can also follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4387.022224