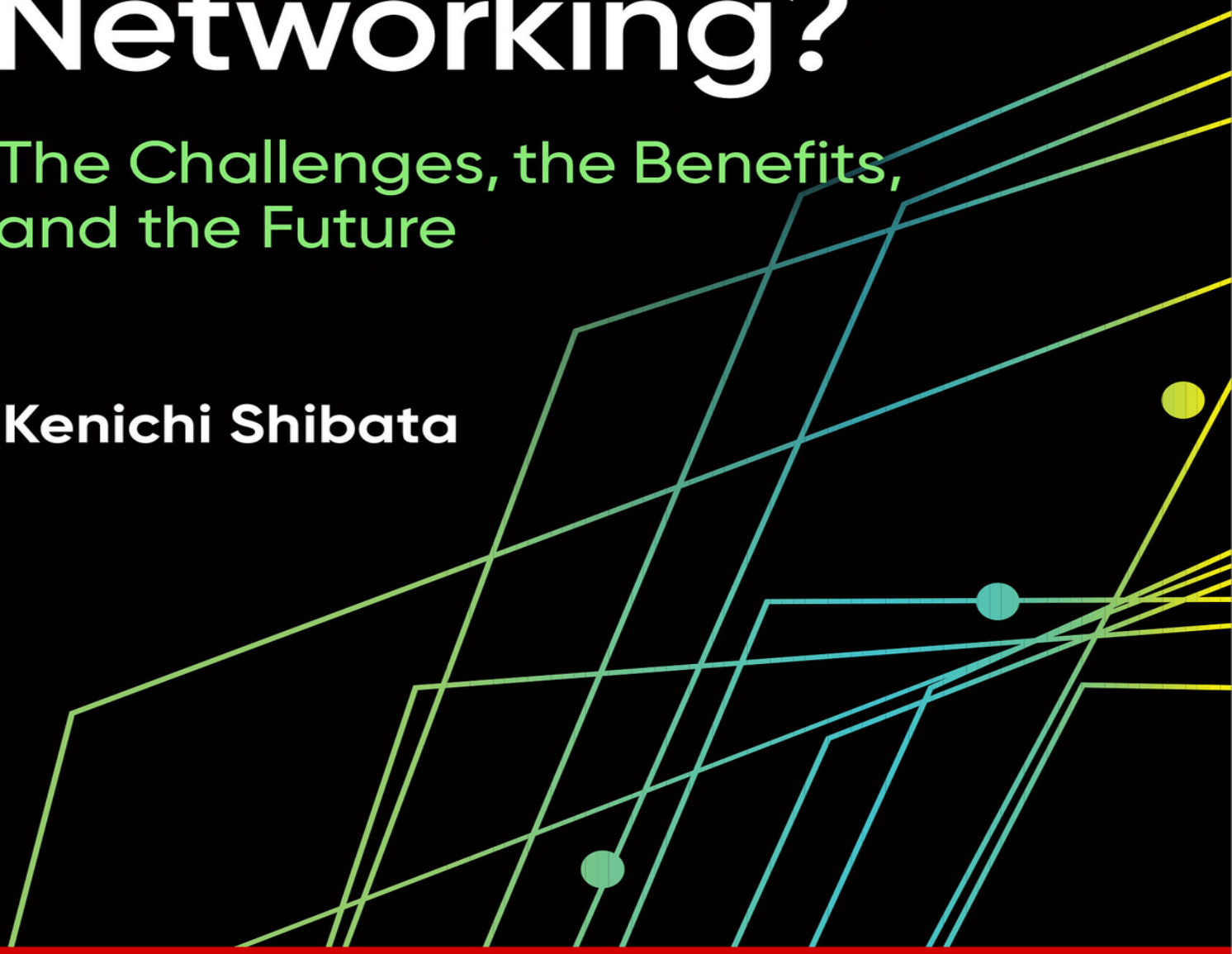
O'REILLY®

Compliments of LogicMonitor

What Is Cloud-Managed Networking?

The Challenges, the Benefits, and the Future

Kenichi Shibata



REPORT

LogicMonitor

LogicMonitor

At **LogicMonitor**, we understand the critical role of network performance in your operations. Whether migrating to the cloud or leveraging IT data, network outages can be tough to manage and quantify.

Traditional network management often introduces complexities that impede business agility, such as distributed configurations, limited visibility, and increased security threats. The rise of remote work, cloud services, and distributed offices requires modern, centrally managed networks.

The Solution: Cloud-Managed Networking (CMN).

Cloud-managed networking (CMN) moves network management to a hosted cloud platform, offering operational simplicity, real-time performance, and security visibility. CMN allows centralized control and visibility of your network, regardless of location. This method focuses on managing any network resource, physical or virtual, from the cloud.

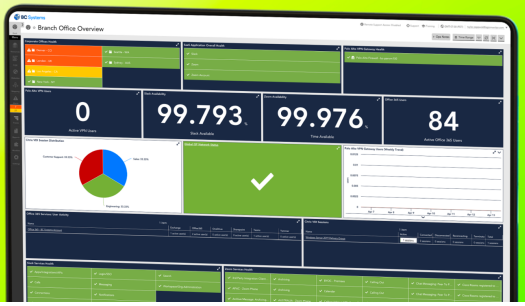
Why Choose LogicMonitor?

LogicMonitor offers a comprehensive observability solution with a single view across your systems, whether on-premise or cloud-managed.

Key Benefits:

- **Unified IT Data:** Single view across hybrid, multi-cloud environments.
- **Kubernetes Visibility:** Insights into topology, performance, availability, and logs.
- **Ease of Use:** Automated discovery, data collection, and thresholding.
- **Over 2500 Integrations:** Ready-to-use integrations with leading cloud-managed SD-WAN and enterprise wireless solutions from Cisco, Ubiquiti, VMware, Palo Alto Networks, Junipter Networks and more.
- **Automated Intelligence:** Forecasting, in-context logs, and AIOps-enabled workflows.

Visit logicmonitor.com for more information.



Contact LogicMonitor today to enhance your network performance monitoring.

What Is Cloud-Managed Networking?

The Challenges, the Benefits, and the Future

Kenichi Shibata

Beijing • Boston • Farnham • Sebastopol • Tokyo

What Is Cloud-Managed Networking?

by Kenichi Shibata

Printed in the United States of America.

Published by O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O’Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://oreilly.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

- Acquisitions Editor: John Devins
- Development Editor: Gary O’Brien
- Production Editor: Gregory Hyman
- Copyeditor: Paula L. Fleming
- Interior Designer: David Futato
- Cover Designer: Susan Thompson

- Illustrator: Kate Dullea

- May 2024: First Edition

Revision History for the First Edition

- 2024-05-07: First Release

This work is part of a collaboration between O’Reilly and LogicMonitor. See our statement of editorial independence.

978-1-098-16491-1

[LSI]

Chapter 1. What Is Cloud-Managed Networking?

Networks form the indispensable backbone of modern organizations. However, traditional network management practices often introduce operational complexities and constraints that impede business agility. The challenges include distributed configurations, time-consuming processes, limited visibility into network health, and increased vulnerability to security threats.

Ensuring optimal network performance requires a high degree of specialized expertise. Network engineers are tasked with configuring and troubleshooting intricate hardware and software components. The constant evolution of security threats demands continual vigilance, a burden that falls on the IT teams responsible for updating and patching network devices on time.

These inherent challenges of traditional networking models are exacerbated in modern IT environments. The proliferation of remote workers, cloud-based services, and distributed branch offices necessitates an adaptable and centrally manageable network. Traditional network infrastructure often struggles to

provide the scalability, flexibility, and unified visibility required to support these dynamic needs.

Cloud-managed networking (CMN) offers a transformative solution designed to overcome the limitations of conventional approaches. Organizations can achieve unprecedented operational simplicity and efficiency by migrating significant portions of management functionality to a hosted cloud platform. This approach promises streamlined network deployment, real-time network performance and security visibility, and a more cost-effective model for meeting evolving business requirements.

This revolution comes with other, underlying changes: cloud manager APIs that observability platforms can leverage, streaming telemetry between devices and cloud-based managers, and constant innovation. A critical and transformational change is sweeping through networks, bringing networking into the cloud era.

It is important to note that CMN is not about hosting virtual network devices in the cloud where they perform network switching and routing functions. Rather, CMN is focused on managing any network resource, physical or virtual, from a cloud-based service. CMN is also not defined by new business

models for network equipment, such as providing equipment as part of a subscription service. However, because subscription equipment services focus on ease of management, they usually include CMN.

This report delves into CMN, exploring its significance and advantages over traditional approaches to management and monitoring.

Cloud-Managed Networking

With cloud-managed networking, some or all network management functions are moved to a cloud-based platform. This allows for centralized control of and visibility into your network infrastructure, regardless of physical location (Figure 1-1).

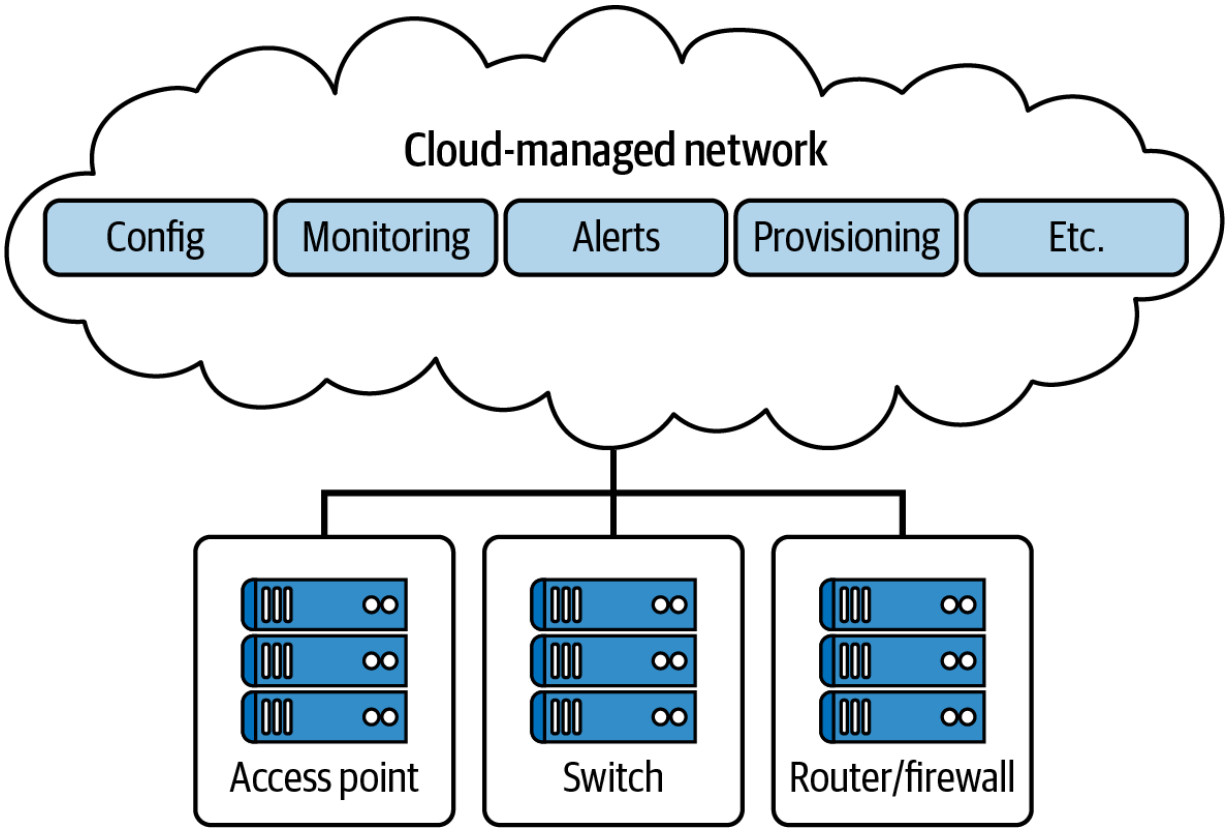


Figure 1-1. A cloud-managed network

A single software service can manage all network devices. Its primary capabilities are configuration and monitoring. Examples of cloud management networking include:

- HPE Aruba Networking
- Cisco Meraki
- Fortinet FortiGate Cloud

The long arc of network management is transitioning from device-by-device management, such as SSH terminal/CLI sessions for each device, to a centralized management solution.

CMN continues that trend, extending the paradigm to cloud-hosted management services. The underlying goal is network management available from any screen, anywhere, at any time, providing analysis and visibility across the entire network as well as ease of operation—including onboarding and ongoing use.

Configuration is improved with centralized configuration management and zero-touch provisioning. Improvements may include enhanced security policies, IP address allocation based on a view of IP allocation over the entire network, wireless parameters, and more.

CMN can be especially ideal for businesses with multiple locations—such as retail chains, banks, and multinational organizations—that want centralized control without replacing their entire infrastructure.

Before Cloud-Managed Networking

The traditional on-premises approach to network management has several inherent shortcomings:

Complexity

Configuring each network device often requires specialized knowledge and complex command-line interfaces, creating a steep learning curve for IT personnel.

Manual processes

Tasks like deploying new devices, updating firmware, or applying security patches is often time-consuming and prone to human error.

Limited visibility

Getting a holistic view of a distributed network can be difficult. Monitoring often involves separate tools and siloed data.

Scaling difficulties

Accommodating growth or rapid changes means purchasing additional hardware, which may then require lengthy installation and configuration cycles.

The Benefits of Cloud-Managed Networking

CMN addresses many of the pain points associated with the traditional model. Here's how the landscape shifts and brings tangible benefits to organizations of all sizes:

Simplified management

Cloud-managed networks have intuitive web-based interfaces accessible from anywhere. This reduces the need for specialized networking expertise and streamlines tasks.

Zero-touch provisioning

New devices can often be added automatically, receiving predefined configurations from the cloud. This makes deployment significantly faster.

Centralized visibility

Real-time dashboards comprehensively overview network health, traffic patterns, and potential security threats.

Enhanced security

Cloud vendors typically push out security updates and patches automatically, helping you maintain a more assertive security posture. With consistent and standardized policies and configurations, network devices

can get security updates and patches simultaneously, further enhancing network security.

Scalability and agility

As a business grows, the number of networking devices that need management increases. With CMN, network resources can be scaled up or down on demand, aligning with business requirements without the lead time associated with procuring hardware. This elasticity allows your network to multiply and support provisioning networking devices at scale.

Streamlined operations

Centralized management, automation, and remote troubleshooting reduce IT teams' workloads, freeing up resources for more strategic initiatives.

Improved flexibility

The cloud model makes expanding into new locations, implementing temporary projects, or adjusting network capacity easier.

Heightened network reliability

Proactive monitoring, automated updates, and a vendor-managed infrastructure can reduce downtime and improve overall network performance.

Improved response times

Network teams can request changes remotely in almost real time without needing on-site interventions, resulting in faster feedback loops, updates, and troubleshooting.

Consistency and standardization

The uniform deployment of policies and configurations across multiple groups of devices and locations allows for a highly consistent network, ensuring that misconfigurations happen less frequently. This consistency also allows for standardized, repeatable deployments, increasing network teams' productivity.

Robust monitoring

With a comprehensive view of network performance, user behavior, and potential security threats from a centralized dashboard, you no longer need to log in to multiple dashboards based on location or device group; everything is centralized in the cloud control plane.

Extensibility

> You can opt in to additional cloud services, such as enhanced analytics, enterprise-level support, and even professional services maintenance, which can function as an extension of your network team.

Financial Transformation

Cloud services transform IT costs from up-front capital expenditure (CapEx) models to pay-as-you-go operating expense (OpEx) models.

CMN relates to the management of network resources and thus explicitly impacts the need to purchase, maintain, and upgrade on-premises hardware and software dedicated to network management. In some traditional scenarios, server hardware has to be upgraded with more memory, for example, before a new software version with new features can be used. This goes away with CMN. New management features can be released every few weeks without the networking team having to touch anything about network management. The up-front cost of hardware and software licenses and ongoing upgrades is replaced with regular OpEx charges aligned with usage.

In a complementary trend, network equipment and virtual appliances are transitioning from CapEx to OpEx/subscription models. The relationship is that equipment provided as part of a subscription service, such as branch wireless devices, is almost always managed with CMN. The promise of a subscription is an easier management experience, and CMN meets this requirement.

Subscription-based network equipment services should not be confused with CMN. However, they usually include CMN (Table 1-1). CMN is applicable to both network resources that are contained in subscription services and equipment that is procured in traditional ways.

Table 1-1. Comparison of cloud-managed networking to non-cloud-managed networking

	CMN	**Non-CMN**
Subscription equipment services	Usually	Unlikely
Traditional equipment procurement	Optional, growing	Traditional

Conclusion

Cloud-managed networking represents a significant step forward for organizations seeking more efficient, scalable, and secure IT infrastructure. While the traditional on-premises model will still have niche applications, cloud-managed solutions are increasingly preferred for businesses of all sizes. Their ease of use, flexibility, and cost benefits make them an attractive option for organizations facing the dynamic demands of the modern digital landscape.

As CMN matures, we can expect even more significant innovations. Tighter integration with other cloud services, advancements in network analytics driven by AI, and simplified software-defined wide area networking (SD-WAN) deployment are likely areas for continued development. The cloud is definitively reshaping the networking world, and organizations embracing this transformation will be well positioned to gain a competitive advantage in future years.

Chapter 2. Adoption of Cloud-Managed Networking

The cloud-managed networking market is substantial and rapidly expanding. Recent estimates suggest it reached a value of $489 million in 2022 and is projected to more than double in size within the next five years.[1] Analysts point to a compound annual growth rate (CAGR) exceeding 20%, indicating exceptional momentum in this sector.

Why Is Cloud-Managed Networking Growing So Rapidly?

Several factors fuel this expansion. CMN's ability to simplify deployment, streamline management, and enhance network security appeals to businesses of all sizes. In addition, the rise of remote work models has accelerated adoption, as has the widespread shift toward cloud-based applications services that demand highly adaptable network solutions.

Technology-centric businesses, born-in-the-cloud startups, and companies with distributed branch offices were among the

earliest to embrace CMN. Their need for agility and centralized management made it a natural fit.

Adoption is now reaching across industries. Retail, healthcare, manufacturing, and even traditionally conservative sectors like finance are increasingly aware of the benefits. The need for agility and reliable network connectivity across numerous locations is driving the expansion of CMN into the mainstream.

CMN dovetails closely with SD-WAN. Many cloud-managed network providers tightly integrate SD-WAN's ability to optimize traffic flow across diverse network links, such as multiprotocol label switching (MPLS) and broadband, driving further adoption as businesses seek to improve their WAN performance.

The vendor landscape is competitive and diverse. Major networking players like Cisco (Meraki), HPE (Aruba), and Juniper Networks (Mist) hold a significant market share. However, innovators like Extreme Networks and niche players specializing in cloud-managed WiFi are also finding success.

Security is of paramount importance, and cloud-managed networking vendors often tout their robust security features. Automatic updates, AI-powered threat detection, and

centralized policy enforcement are crucial aspects of vendor selection, influencing continued adoption.

Use Cases for Cloud-Managed Networking

Cloud-managed networks have become increasingly popular due to their scalability, flexibility, and ease of management. Here are some use cases that highlight the benefits and applications of CMN:

Scalable WiFi infrastructure projects

There is a growing need for a WiFi infrastructure refresh and installation in many sectors, such as retail, healthcare, higher education, financial services, and even pharmaceuticals. WiFi improvements enhance customer experience and improve the digitization of business services. CMN enables easy deployment, management, and scaling of WiFi networks through integrated, scalable CMN devices managed centrally via the cloud.

SD-WAN initiatives for private WAN security

Regulated industries, such as financial services, require reliable connectivity and security. By integrating SD-WAN with CMN solutions, businesses can effectively manage network connectivity with security and reliability in

mind. This leads to improved business services, streamlined performance, and improved protection.

Multilocation business operations

Businesses with multiple office locations can use CMN to unify their communication systems, streamline data sharing, and ensure consistent security policies across all sites. This facilitates seamless collaboration and resource access, regardless of geographic location.

Remote work enablement

Cloud-managed networks are ideal for supporting remote or hybrid work models. They allow employees to securely access corporate resources from any location, using any device, enhancing productivity and flexibility without compromising security.

Scalable IT infrastructure for startups and small-to-medium enterprises

Small and medium-sized enterprises (SMEs) and startups can benefit from the scalability of CMN. As these businesses grow, they can easily add new users, devices, and locations without significant capital investment in physical infrastructure.

Seasonal business demands

Cloud-managed networks allow for easy scalability by businesses with fluctuating needs, such as retail companies that experience sales surges around holidays. They can adjust bandwidth and network services to accommodate increased demand and then scale down as required.

Disaster recovery and business continuity

Cloud-managed networks can be crucial in disaster recovery and business continuity plans. By leveraging cloud resources, businesses can ensure that critical data and applications remain available, even in the event of a local failure.

Security and compliance management

Companies subject to strict regulatory requirements can use CMN to simplify compliance. Centralized management features allow for consistent application of security policies, regular updates, and detailed reporting to meet compliance standards.

Temporary workspaces and pop-up events

Cloud-managed networks are well-suited for temporary events like trade shows, pop-up stores, or construction sites, providing rapid network infrastructure deployment with minimal physical setup.

Internet of Things (IoT) applications

In sectors like manufacturing or agriculture, CMN facilitates connecting, monitoring, and managing vast arrays of IoT devices, enabling real-time data collection, analysis, and action.

Industry-Specific Use Cases for Cloud-Managed Networking

The following use cases demonstrate the versatility and benefits of CMN across various industries, highlighting its ability to enhance connectivity, security, and operational efficiency:

Retail chain management

Retail businesses with multiple locations can benefit greatly from cloud-managed networks. CMN allows for the centralized management of WiFi access points, payment systems, inventory databases, and surveillance cameras across all stores. Network configurations can be

standardized and deployed remotely, ensuring uniform customer experiences. Additionally, these networks can gather data to provide insights into customer behavior and store performance.

Educational institutions

Schools, colleges, and universities can leverage cloud-managed networks to provide secure and scalable internet access to students and staff across campuses. CMN supports online learning platforms, library databases, and administrative operations. It also facilitates the segmentation of networks for different users (e.g., students, faculty, guests) and the prioritization of educational resources to ensure smooth online learning experiences.

Healthcare facilities

In healthcare, cloud-managed networks support the increasing use of telemedicine, electronic health records, and mobile medical devices. They ensure secure and compliant data handling, facilitate seamless communication among medical professionals, and enable remote patient monitoring. Network scalability is crucial

for handling varying loads of patient data and ensuring network availability for critical care.

Event management

For temporary events like conferences, trade shows, and music festivals, CMN allows for quick deployment of WiFi networks to accommodate varying numbers of users. Organizers can monitor network performance in real time, adjusting bandwidth allocations as needed to ensure high-quality connectivity. Post-event, the networks can be easily decommissioned or repurposed for future events.

Smart city initiatives

Cloud-managed networks are crucial in smart city development, connecting sensors, cameras, and IoT devices across urban areas. They facilitate data collection and analysis for traffic management, public safety, and environmental monitoring. Cloud management enables city administrators to scale network infrastructure as the city grows and to apply updates and security patches centrally.

Hospitality industry

Hotels and resorts use cloud-managed networks to provide guests with seamless WiFi access while securing backend systems and guest data. Network administrators can create personalized experiences, such as custom login pages, and gain insights into guest preferences. Additionally, they can manage network access for different areas, such as guest rooms, conference centers, and public spaces, from a single platform.

Challenges of Cloud-Managed Networking

Adopting CMN brings numerous benefits, but organizations might face challenges, including:

Security and privacy concerns

One of the most significant challenges is ensuring data security and privacy. Moving network management to the cloud requires transmitting and storing sensitive information off-site, which can raise concerns about data breaches, loss of control over data, and compliance with regulations like the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA).

Legacy system integration

Integrating CMN solutions with existing legacy systems can be complex and time-consuming. Organizations often have significant investments in traditional infrastructure, and transitioning can involve compatibility issues, data migration challenges, and the need for staff retraining.

Performance and bandwidth limitations

Moving network management functions to the cloud can introduce latency, especially for geographically dispersed organizations. Ensuring sufficient bandwidth and optimizing network performance can be challenging, particularly in areas with limited connectivity options.

Change management

Transitioning to CMN involves changes in processes and potentially organizational structure. Resistance from employees accustomed to traditional networking setups can hinder adoption and must be overcome with effective change management strategies.

Compliance and legal issues

Navigating the complex landscape of international laws and industry regulations regarding data protection, storage, and transmission can be difficult. Compliance

becomes especially challenging when dealing with cloud providers that operate across multiple jurisdictions.

Business continuity and disaster recovery

While cloud-managed networks can support business continuity planning, relying on third-party providers means that organizations must ensure that their chosen providers have robust disaster recovery plans.

Hybrid IT and Cloud-Managed Networking

Many networking teams find themselves working in hybrid IT environments, as their companies have not fully migrated to the public cloud. In addition, networking inherently involves physical devices at branches and other locations, even if the company is not operating data centers. Although hybrid IT has benefits, its additional complexity warrants dedicated attention.

What Is Hybrid IT?

Hybrid IT (Figure 2-1) is an approach to IT infrastructure that combines a mix of:

On-premises resources

These include traditional data centers or servers you own and manage within your physical location.

Private cloud

Private cloud resources (e.g., servers, storage, networking) are dedicated solely to your organization. These might be in your own data center or hosted by a provider.

Public cloud

Public cloud resources are procured from major providers like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. These are shared with other customers but offer high scalability and a pay-as-you-go cost model.

The key to a successful implementation of hybrid IT is that these components are designed to work together seamlessly, allowing you to place workloads in the environments best suited to them.

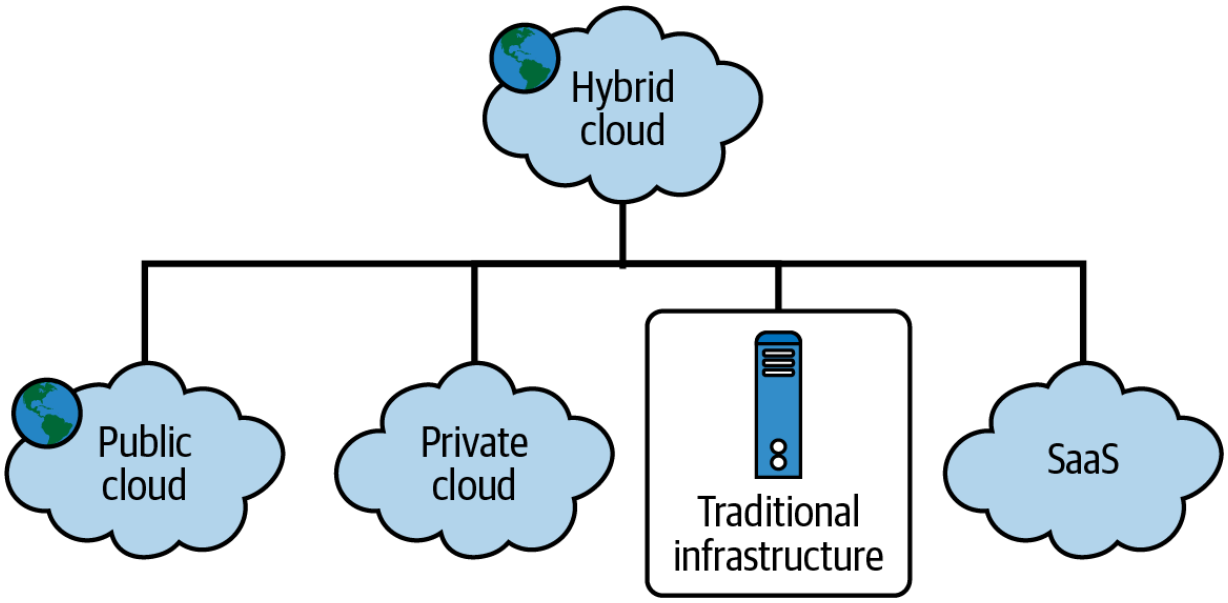


Figure 2-1. An example hybrid IT infrastructure

Why Hybrid IT?

There are several benefits of hybrid IT, including:

Flexibility

Match workloads to the ideal environment based on performance, security, or cost needs. This gives you more options than relying solely on one type of infrastructure.

Control

Keep sensitive data or systems with strict compliance needs on-premises while leveraging the cloud for other workloads.

Cost optimization

The public cloud is great for scalability and handling unpredictable traffic spikes, but running certain stable workloads in-house might be more cost-effective.

Gradual cloud migration

Shift to the cloud at your own pace, testing and migrating workloads over time instead of using an all-or-nothing approach.

Leverage existing investments

If your data center has recently been refreshed, hybrid IT lets you maximize that investment while still taking advantage of the cloud.

Hybrid IT Considerations

As mentioned earlier, hybrid IT requires more attention to detail than other setups. It's important to consider:

Complexity

Managing a hybrid environment can be more operationally complex than managing a single-location or cloud-only approach.

Integration

Ensuring that data and applications work seamlessly across on-premises and cloud systems requires careful planning and tools.

Visibility

Monitoring performance and security across a hybrid landscape might require dedicated tools or centralized dashboards.

Skills

Your IT team may need a mix of traditional data center expertise and cloud skills to be successful with hybrid IT.

Cloud-Managed Networking for Hybrid IT

Hybrid cloud and cloud-managed networking complement each other, offering a cohesive approach to modern IT challenges. Hybrid cloud environments can be more effectively managed and optimized with CMN solutions. Here's how they work together:

Unified management across environments

CMN can span across the hybrid cloud, offering unified network management regardless of whether resources are in the public cloud, private cloud, or on-premises.

Enhanced performance and efficiency

CMN tools can optimize the performance of hybrid cloud applications by managing traffic flows, balancing loads, and reducing latency.

Improved security posture

A cloud-managed network solution can enforce consistent security policies across the hybrid cloud environment, ensuring secure data transfers between cloud services and on-premises resources.

Seamless connectivity and integration

CMN facilitates the seamless integration of public and private clouds, ensuring reliable connectivity and smooth operation of applications and services, regardless of where they reside.

In summary, while hybrid cloud offers a flexible and secure approach to enterprise IT infrastructure, CMN provides the tools and capabilities to manage this complex environment

efficiently. Together, they enable businesses to be more agile, secure, and competitive in today's digital landscape.

Cloud-Managed Networking Adoption

The rise of the cloud created the opportunity to invest in a long-term, scalable solution that requires fewer internal resources.

CMN is increasingly being adopted by smaller and midsized enterprises. Since CMN provides a manageable solution that does not require dedicated staff, it is a good choice for SMEs, which often lack the IT and infrastructure staff that big companies possess.

CMN is also widely adopted by big enterprises, largely due to its scalability, centralized control, flexibility, and security.

Practical Implementation of Cloud-Managed Networking

As adoption of CMN increases, the practicalities of implementation are as critical as the conceptual considerations. This is particularly evident when migrating traditional network

management systems to CMN solutions. For example, most large enterprises using Cisco use Cisco Prime. To illustrate such a migration, we will use a scenario in which an organization migrates from Cisco Prime to Cisco Meraki.

Transitioning to a CMN system like Cisco Meraki offers advantages such as long-term cost savings and bolstered security. A successful migration depends on adequately upskilling the company's network engineers and establishing processes that leverage the strengths of the CMN model. Once these milestones are achieved, network challenges can be addressed more effectively, allowing for more efficient and secure networking.

There are several key challenges you'll need to keep in mind:

Skills gap

Traditional network skills do not automatically translate into expertise in cloud technologies, including CMN. For example, Cisco Prime relies heavily on local command-line configurations. Migration to Meraki, which utilizes a centralized control plane GUI, requires climbing a steep learning curve. A persistent skills gap can lead to misconfigurations or the underutilization of key features.

Configuration variances

Network configurations are implemented differently in Cisco Prime and in Meraki. For example, quality of service settings, VLAN configurations, and access control lists have different implementation nuances.

Security transition

Prime has only non–cloud security features, while Meraki has robust cloud security features such as cloud-based threat detection, encryption, and access control mechanisms. Adopting and correctly configuring these features may prove challenging.

Data security concerns

Moving to CMN raises concerns about data security. Ensuring segmentation, end-to-end encryption, and compliance with regulatory requirements is of paramount importance during migration.

Licensing and support

Prime and Meraki have different licensing models. Transitioning will involve revisiting licensing and support agreements.

How to Choose the Correct Technology

When modernizing your network, the starting point is always to understand your organization's specific needs. For instance, a business with a heavy data load, such as a media company, would benefit from Cisco's Meraki MX because of its robust bandwidth management. Alternatively, an event management company that frequently changes its network configuration might find the adaptability of HPE Aruba's SD-Branch more suitable.

In the CMN landscape, Cisco, Fortinet, and HPE each bring its own strengths. Cisco's Meraki has a user-friendly interface, scalability, and extensive cloud management capabilities that are ideal for those who prioritize ease of use and comprehensive control. Fortinet's FortiGate stands out in security, making it a top choice for industries such as finance or healthcare. Finally, HPE's Aruba may be a good choice when you need flexibility and focus on edge technologies. Aruba devices are often deployed when you have IoT devices that require flexibility and mobility for the business to securely connect and get insights from a range of data sources.

The choice among Cisco, Fortinet, and HPE for your CMN solution hinges on balancing existing infrastructure, cost,

scalability, security, and performance:

Integration and compatibility

Does your current network infrastructure include hardware from specific vendors? How will the new technology integrate with it? For a network with existing Cisco hardware, opting for Meraki can make integration seamless. However, in an environment with a mix of different vendor equipment, Aruba's flexible solutions can be a game-changer, allowing for a more diverse network setup.

Cost considerations

What is your budget for immediate implementation, and what are the expected long-term operational costs? Cost is always a crucial factor. While Cisco's solutions might seem pricier up front, they often offer a lower total cost of ownership due to their durability and ease of management. Fortinet, meanwhile, might suit those looking for budget-friendly options without having to compromise on security features.

Scalability and future growth

Ask yourself, how much data do you need to handle? What are the peak load times? For media companies and other organizations with heavy data loads, Cisco Meraki, with its scalability and robust bandwidth management, is ideal.

A growing business needs a network that grows with it. Both Meraki and Aruba excel in scalability, but your choice might depend on the specifics of your expansion plans. Aruba is particularly adept at accommodating rapid and diverse device management needs, while Cisco stands out for its enterprise-grade scalability, robust bandwidth management, and low latency performance.

Security

Reflect on what level of security your network operations require. Are you in an industry with stringent data security needs? In an era where cyber threats loom large, the robust security features of Fortinet's solutions, such as intrusion prevention, stateful packet inspection, and application control, can provide peace of mind, especially in data-sensitive sectors such as banking and healthcare.

Real-world trials

> Before finalizing your decision, consider conducting pilot tests with selected technologies. Real-world testing can offer invaluable insights that specification sheets and sales pitches cannot match.

Conclusion

The cloud-managed networking market is experiencing rapid growth, with projections indicating it will potentially double in size within the next five years. This expansion is driven by the ability of cloud-managed networking to simplify deployment, enhance security, and streamline network management. Businesses of various sizes are adopting this technology, and its integration with SD-WAN further supports its growth. The vendor landscape includes major players like Cisco Meraki, HPE Aruba, and Fortinet, as well as niche providers.

CMN offers advantages across various industries. These include scalable WiFi infrastructure, SD-WAN for secure private networks, management for multilocation businesses, and support for remote work models. Its scalability is particularly appealing to startups and SMEs. Cloud-managed networks also play a role in disaster recovery, compliance, and temporary or IoT-heavy deployments. Use cases are diverse, with specific

examples found in sectors such as retail, healthcare, education, event management, and hospitality.

CMN solutions offer a compelling complement to hybrid IT environments. Organizations benefit from unified management across on-premises, private cloud, and public cloud resources. They can optimize application performance and enhance security posture when workloads are distributed. CMN allows seamless connectivity and integration across these environments, supporting businesses that need both the flexibility of the cloud and the control of on-premises infrastructure.

- Mark Leary, “Worldwide Enterprise Network Observability Forecast, 2023–2027,” IDC, December 2023, *https://www.idc.com/research/viewtoc.jsp?containerId=US51409223*.

Chapter 3. Monitoring Cloud-Managed Networking

While adopting cloud-managed networking is itself a significant change, CMN also tends to drive other changes in the organization's technology environment. For example, organizations often complement CMN by making greater use of streaming telemetry and integrations with network managers.

Underlying Changes Driven by Cloud-Managed Networking

Organizations that adopt CMN often also begin collecting data in new ways. For example, streaming telemetry, which is available on many devices but rarely used, is becoming increasingly popular with CMN because it is effective for cloud-based management.

Integration with a centralized network manager, such as Cisco Catalyst Center or Aruba Central, is also growing in popularity. Such integrations provide significant advantages, but existing tools may continue to support the option to collect directly from

network resources as well. Whether to integrate and when are key considerations for networking teams.

We'll explore both of these essential changes in the following sections.

Streaming Telemetry

Streaming telemetry is a network-monitoring approach in which devices continuously push real-time data (e.g., metrics, state information, events) to a central collector, often using a publish–subscribe model. This contrasts with traditional polling methods, like Simple Network Management Protocol (SNMP), in which data is requested at intervals. Streaming telemetry provides several advantages:

Real-time visibility

: Streaming telemetry provides near-instant insights into network health and performance. You can detect problems as they occur, not minutes or even hours later.

Granular data

: Streaming telemetry often captures a broader range of data points at higher frequencies than do polling

methods. This enables more detailed analysis for troubleshooting or capacity planning.

Proactive problem resolution

Real-time alerts about traffic spikes, interface errors, and security events let you take corrective action before such events escalate into significant outages.

Streaming telemetry can be pushed to any destination. However, one use case specifically applies to CMN: pushing telemetry to a network manager.

As Figure 3-1 shows, Cisco Catalyst Center receives data pushed to it from devices using streaming telemetry. Cisco Catalyst Center then provides the telemetry data to other observability solutions through its intent-based API. While Figure 3-1 shows wireless controllers and access points, Cisco Catalyst Center supports a range of Cisco equipment, including switches and routers.

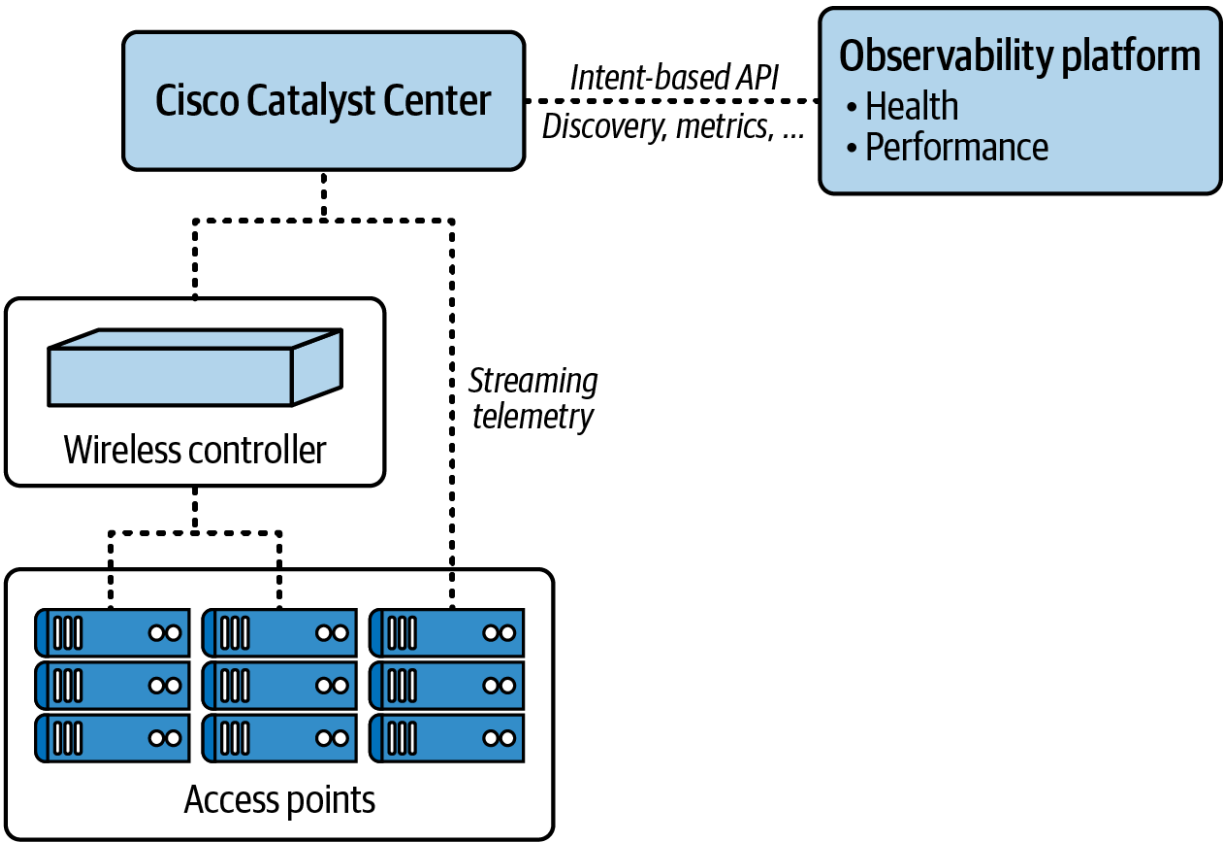


Figure 3-1. Streaming telemetry with Cisco Catalyst Center

Integrating with a Network Manager

With additional tooling capabilities, such as multivendor observability, you can realize many benefits from integrating with network managers like Cisco Catalyst Center and Aruba Central. These include:

- Faster device discovery
- Faster time to observability

Device discovery helps other tools work faster because the network manager has already completed this task, meaning that additional collectors or agents do not have to be deployed to do discovery.

There are tradeoffs, though. The integration API provided by the network manager may not offer the same granularity of information as does regular device polling. On the other hand, alerts and updates may be more timely. Depending on the tool, support for devices that directly poll the data may need to be retained. If so, it should be capable of operating at the same time as integrations with network managers.

It is important to note that as equipment vendors focus more on streaming telemetry, their support for SNMP-provided data may decline. For this reason, it is essential that tooling support integrations with new cloud-era managers. This is true whether they are operating on-premises or as a software as a service (SaaS).

Monitoring Cloud-Managed Networks

As discussed in Chapter 2, hybrid IT infrastructure usually means that workloads can simultaneously be on-premises and in one or more private and/or public clouds, and more commonly they migrate between on-prem and cloud as needed. The more systems one has to interface with to get the "full picture," the more complicated the infrastructure is.

Businesses must consider hybrid monitoring solutions that operate seamlessly across both on-premises and cloud environments. These solutions should provide comprehensive network performance and security monitoring, as well as facilitate effective data exchange and operational stability between on-premises and the cloud.

Key features for effective hybrid monitoring must support the following data types:

SNMP

: Available in both CMN and traditional networking devices

REST API

: Available in both CMN and traditional networking devices

Streaming telemetry

: Increasingly used by CMN devices

Webhooks

An option for CMN devices

Because hybrid IT infrastructure is highly interdependent, monitoring solutions must bridge the gap between the cloud and on-premises components. This requires tracking the performance and stability of each component and understanding how all elements interact with each other and behave as a whole. An integrated monitoring solution is crucial for detecting and resolving issues arising from the dynamics of an architecture that spans the on-premises and cloud environments.

To understand CMN monitoring at a high level, it is crucial to identify the scope and scale of the network you're monitoring. This includes understanding the geographic distribution of network resources, the scale of operations, and the variety of devices and services integrated into CMN. Recognizing these factors will help you tailor a monitoring plan that aligns with the specific needs and challenges of the network.

CMN monitoring must be able to continuously monitor the network's performance and availability over time. It must effectively track the network's state (status), statistics (performance metrics), and events (significant occurrences or

changes in the system) to provide a holistic view of the network's health. This multidimensional monitoring ensures that the network operates optimally.

The Key Components of a Cloud-Managed Networking Monitoring Solution

CMN represents a shift from monitoring individual devices to establishing a detection-and-response model of the entire network, allowing for a more holistic approach to monitoring networks. As shown in Figure 3-2, monitoring in CMN moves away from getting every telemetry data point from every device and toward alerting only if there is an issue with a device (e.g., the network switch fans).

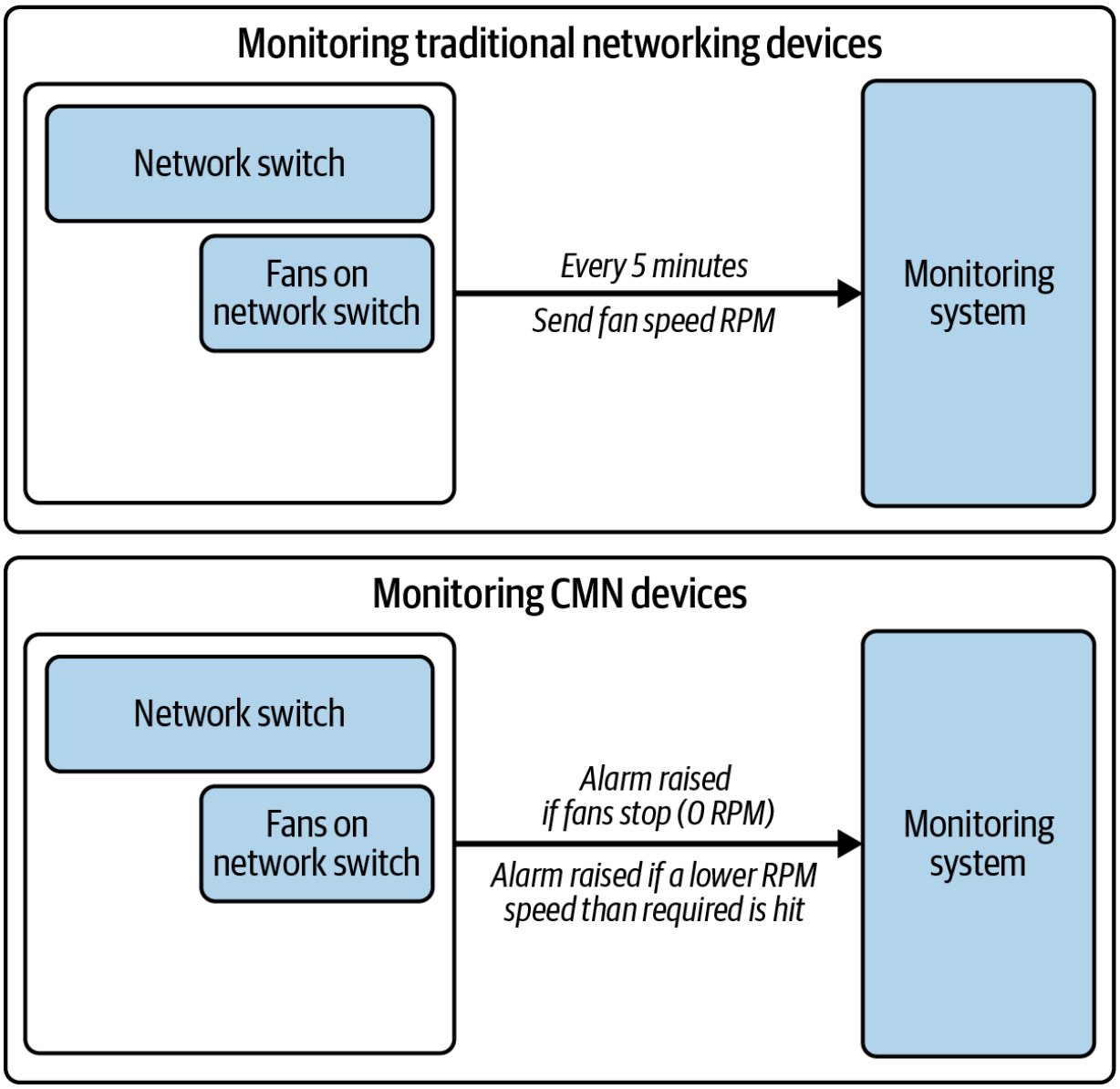


Figure 3-2. Example of monitoring the network switch fans in a traditional system and with CMN

As networks transition to CMN, the relevance of device-specific monitoring decreases. This makes it necessary to reevaluate critical components of network monitoring. A centralized monitoring solution needs the following elements:

Customer subscription

Be aware of when the CMN subscription will expire. Unlike in traditional networking management, your CMN devices will stop working once your subscription runs out.

Broad vendor and device support

The capability to ingest various data types, including metrics, logs/event flows, and configurations, from a diverse group of CMN devices is key. This extensive data support facilitates a deeper and more nuanced comprehension of network functions.

Cloud platform monitoring

You should be able to monitor the configuration changes of the tenant in CMN. For example, if someone changes something on the device configurations of Cisco Meraki, these changes need to be monitored and added to the dashboard. This brings us to another key component.

Customizable dashboards and reporting tools

Customizable dashboards and reporting tools are essential for visualizing network data and gaining actionable insights. These tools should offer the flexibility

to tailor views and reports according to specific requirements, ensuring that network administrators have the information they need at their fingertips.

Robust security and compliance monitoring

Given the critical importance of security in CMN, monitoring solutions must include robust security and compliance features. These features must be able to detect and respond to security threats in real time and ensure that the network remains compliant with relevant regulations and standards.

Advanced monitoring

The adoption of advanced monitoring tools can support CMN operations. Organizations must stay ahead of the evolving networking landscape to maintain optimal performance and reliability of their cloud-managed networks. Because network data is often large and needs to be processed and correlated, advanced monitoring technologies are needed.

Embracing Advanced Monitoring Technologies

The use of advanced monitoring technologies such as cloud-based network analytics, autogenerated topology mapping, machine learning–based anomaly detection, and data forecasting can lead to better CMN monitoring outcomes.

These advanced monitoring technologies enable organizations to manage and analyze large volumes of network data efficiently, identify potential issues before they escalate, and automate response mechanisms for rapid problem resolution. Additionally, these solutions can better integrate with cloud APIs and other digital transformation technologies, ensuring seamless operation in a hybrid cloud environment. We explore several of these here:

Dynamic device discovery

Dynamic device discovery is an essential monitoring capability in CMN. The deployment of CMN devices is commonly streamlined through zero-touch provisioning (ZTP). ZTP simplifies network expansion and maintenance. Devices are shipped directly to sites and, upon arrival, plugged in without any need for specialized network knowledge. Initiating setup is simple; it involves basic steps like connecting cables to designated ports and waiting for a confirmation signal, such as a solid green LED, to indicate successful activation.

However, dynamic discovery is needed to monitor these devices. Dynamic discovery enables us to discover and monitor new devices as they come online or to find an entire enterprise or select sites without deploying a collector at each site.

Cloud-based network analytics

Networking engineers often debate whether network analytics should be performed in the cloud or locally. Placing the analytics engine in the cloud offers access to more processing power and communications with other networks. Cloud-hosted analytics also benefit from up-to-date algorithms and crowdsourced data.[1]

Autogenerated topology mapping

Topology mapping is the visual representation of relationships among elements within a communications network.[2] In CMN, where network devices can be provisioned and deprovisioned at a moment's notice, topology mapping is absolutely critical. Since networks in CMN are extensive, autogenerated or dynamic discovery is essential. Viewing individual connections should be additive, and visualizations should be done on the fly to aid discovery.

Anomaly detection and data forecasting

Anomaly detection identifies data that does not conform to expected (or usual) patterns.[3] Anomaly detection systems employ machine learning algorithms to recognize and learn from established data patterns. This can enable the system to identify and flag anomalies in resource behavior, providing insights that can prevent issues from escalating. For example, triggering automatic alerts when data deviates from expected patterns and visually emphasizing forecasted data ranges on graphs makes it easy to spot any data that deviates from the norm.

Data forecasting allows you to predict future trends for your monitored infrastructure, using past performance as a basis.[4] The process involves identifying anomalies and missing data and then applying a capacity-trending algorithm to identify the best-fit model for the existing data. You then use this model to calculate future trends.

Key Metrics for Cloud-Managed Networking

When it comes to CMN, monitoring key metrics is essential to ensure network health and performance. CMN environments

typically include routers/firewalls, switches, and access points (APs), each with specific key performance indicators that must be tracked.

Router/firewalls

For routers and firewalls, monitoring focuses on several critical aspects:

Status of LAN and WAN ports

Ensure that these are operational and identify any connectivity issues.

WAN metrics

This includes monitoring the percentage of WAN utilization, packet loss, jitter, and latency. Tracking these metrics is crucial for maintaining optimal network performance.

Failover events

Monitoring the failover from one ISP to another or from one port to another helps to ensure the continuity and reliability of network connectivity.

NetFlow data

Analysis of network traffic flow enhances understanding of traffic patterns, bandwidth usage, and potential bottlenecks.

Security event

Particularly for firewalls, monitoring every transaction is vital for security and threat detection.

Access points

Key metrics for APs include:

Network health and availability

This includes the status and performance of service set identifiers (SSIDs), wireless networks, and virtual APs.

Radio performance and utilization

It is necessary to monitor the performance and utilization of each radio frequency band (2.4Ghz, 5Ghz, and 6Ghz for the newer 6E standard).

User count

Tracking the number of users per radio frequency and per SSID is crucial for capacity planning and troubleshooting.

Packet loss

Identify packet loss to ensure data integrity and network efficiency.

Association and authentication issues

Monitor for any issues in device connection and network access.

Switches

For switches, key metrics to monitor include:

Port status

Monitor the state of each switch port to detect any failures or disconnections.

Packet loss (discard rate)

Identifying packet loss on each port can indicate congestion or hardware issues.

Error rate

Monitor for errors in data transmission to maintain data integrity.

Transmission and reception statistics

Analyze the amount of data transmitted and received through each port.

Port utilization

Understand how much capacity is being used on each port to manage network resources effectively.

Vendor-specific metrics

Some vendors, like Cisco Meraki, might not provide traditional metrics like CPU, memory, and disk utilization. Instead, they offer alternative indicators, such as a health score that assesses the overall status of network devices. These vendor-specific metrics provide a more holistic view of device performance and health, aligning with the organization's needs with CMN.

Conclusion

In summary, CMN marks a significant evolution in network management, and it demands new integrations to fully harness its benefits. Effective CMN monitoring goes beyond traditional methods, requiring adaptation to CMN's dynamic and distributed nature. Organizations can ensure robust, compliant,

and efficient network operations by embracing new monitoring technologies.

- "What Is Network Analytics?" Cisco, accessed December 22, 2021, *https://www.cisco.com/c/en/us/solutions/analytics/what-is-network-analytics.html*.

- "Topology Mapping Overview," LogicMonitor, updated March 29, 2024, *https://www.logicmonitor.com/support/forecasting/topology-mapping/topology-mapping-overview*.

- "Anomaly Detection Visualization," LogicMonitor, updated January 7, 2022, *https://www.logicmonitor.com/support/forecasting/anomaly-detection/anomaly-detection-visualization*.

- "Data Forecasting," LogicMonitor, updated March 27, 2020, *https://www.logicmonitor.com/support/forecasting/overview/data-forecasting*.

About the Author

Kenichi Shibata is a cloud native architect and software engineer with extensive experience in designing, implementing, and managing scalable systems using microservices, cloud infrastructure, and high-throughput web applications and APIs. His experience spans multiple industries, including fintech, insurance, and finance in Japan and the UK, where he has utilized technologies such as Python and NodeJS to develop high-stability, high-throughput systems.