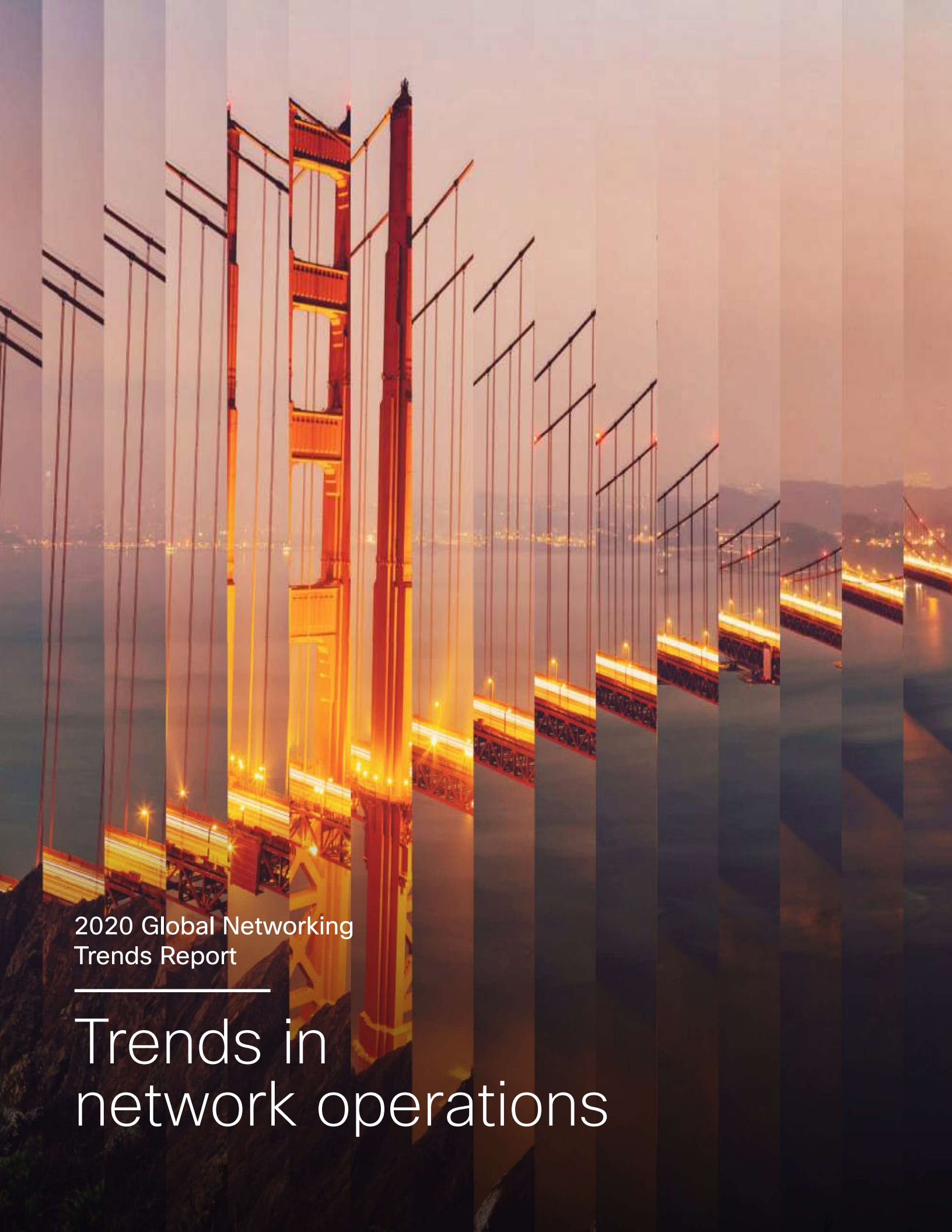


2020 Global Networking Trends Report

Trends in network operations

Transitioning from reactive to business optimized

Section summary

Key takeaways

- Traditional network operations models are not sustainable to support the required business services in the face of ever-increasing digital demands.
- IT teams are modernizing IT operations and adopting DevOps approaches to leverage controller-based systems and AI-enabled tools that automate or eliminate many traditionally repetitive network tasks.
- New advanced open-network platforms enable better integration into other IT and security systems and operational processes and provide new opportunities for business application developers.
- In this next era of network operations, leaders and teams will be better positioned to move away from reactive operational models and continuously deliver the precise services that the business needs.

Key findings

- 73% of teams spend more than half their time just maintaining the status quo of the network.
- IT leaders would prioritize their network teams' resources to focus on multicloud; accelerate application deployments; and better protect the network, applications, and data if they could free up resources from daily maintenance tasks that "keep the lights on."
- More than a third of IT leaders prioritized the importance of achieving better network coordination and integration with other IT teams and lines of business.

Section summary (continued)

Essential guidance

- When adopting controller-based automation and assurance models, networking teams should focus their efforts on three critical process areas: lifecycle management, policy management, and assurance management.
- To improve service quality, cost, agility, and security, network administrators should move away from managing individual devices and focus their attention on the network controller and managing the end-to-end network system via the controller.
- Networking teams should embrace an open-platform, DevOps-led approach to integrate the network into IT processes and streamline end-to-end workflows so they can gain efficiencies and be more responsive to business needs.
- Network operations teams should equip themselves with emerging AIOps capabilities to deliver better network and business outcomes.

Top predictions

Bridging business and IT: "Teams will rebalance time spent maintaining networks toward an outward focus on how the network can better meet organizational needs and support business innovation. New operations roles will be chartered with translating business intent and application requirements into network policies."

NetOps extending monitoring to the cloud: "As multicloud business services become the norm, NetOps teams will extend visibility and predictive monitoring across WAN, public networks, and to the cloud point of presence. For even greater insights, enterprise intent-based networking systems will start integrating data from service provider and cloud provider systems to ensure continuous quality of experience for cloud services."

– Rich Plane, CTO of Customer Experience, Cisco

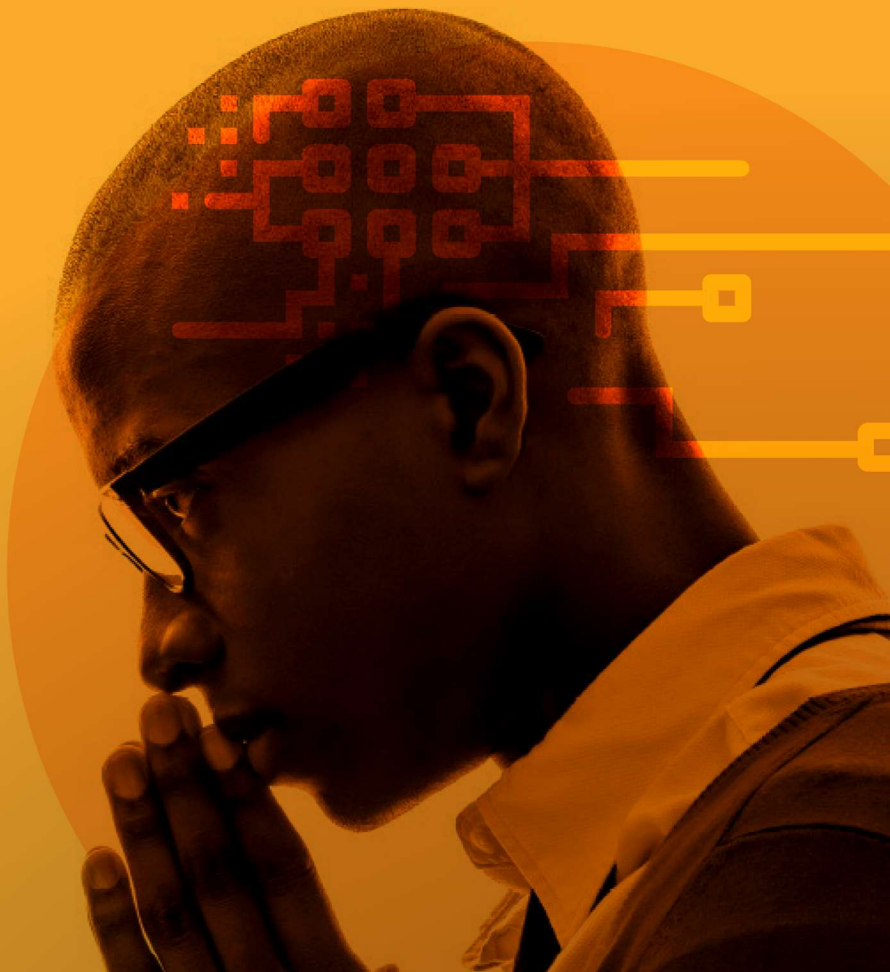
Transitioning from reactive to business optimized

According to Cisco research, IT leadership teams are spearheading the digital transformation for their organizations. To accomplish this, they are driving a separate but equally important transformation—that of modernizing IT infrastructure and operations to meet emerging digital demands.[34]

For the first time, networking teams—by virtue of embracing an open-platform, DevOps-led approach—have the tools and technologies to integrate the network into IT processes and streamline end-to-end workflows so they can gain efficiencies and be more responsive to business needs.

This approach also provides an opportunity to build operational bridges between network domains as well as integrate directly with applications to better support the changing needs of the lines of business.

By adopting new ways of thinking about network operations and new ways of working, IT leaders and teams will be better positioned to deliver the exact services that lines of business need, whether better existing services or new business-enabling services.



63%

According to our *2019 Global Networking Trends Survey*, 63% of IT leaders plan to put in place advanced networks that can dynamically meet business needs within three years.[14]

Current and future state of network operations

Operational readiness to support digital transformation

In our *2019 Global Networking Trends Survey*, we asked IT leaders and network strategists how they would classify their current network operational readiness with regard to assurance management across five stages of maturity ranging from reactive to business optimized.

While only 23% currently consider themselves to be predictive or business optimized, 71% plan to be there in two years, underscoring the urgency that organizations feel in preparing for increasing demands on the enterprise network.[14]

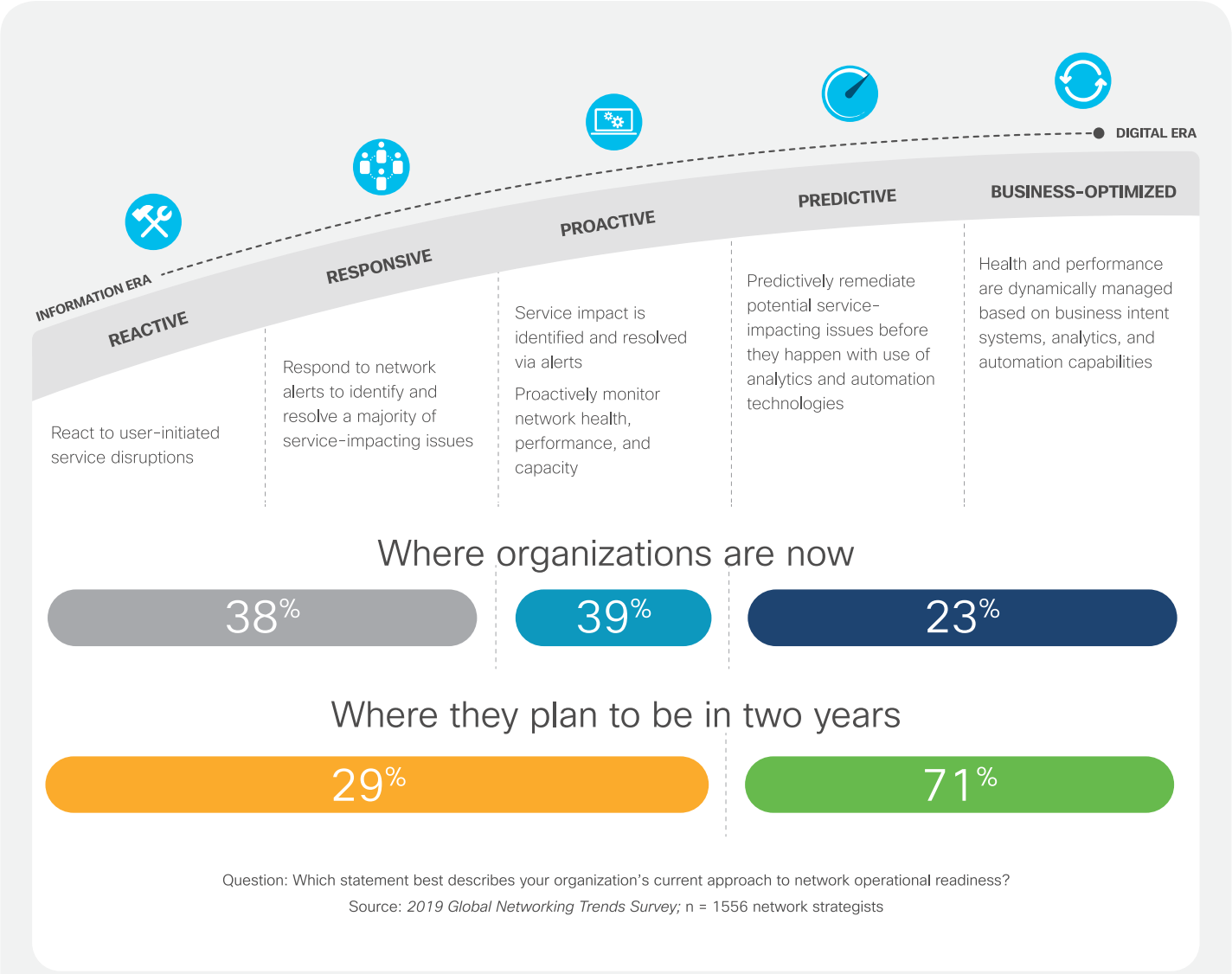
How network advances are changing network operations

The recent surge of advanced network technologies will change virtually every aspect of network operations, and major changes can be expected in the following areas.

Network operations integration into the IT process

The old days of networks being operated in technology silos by engineers with expertise primarily in one area are fading fast. In our research, almost one-third of IT leaders emphasized the importance of achieving better network coordination and integration with other

Figure 25 Network operations readiness: Assurance management



Question: Which statement best describes your organization's current approach to network operational readiness?
Source: *2019 Global Networking Trends Survey;* n = 1556 network strategists

IT teams, while 26% revealed the importance of improving their ability to engage with lines of business.[14] An additional 27% identified that a siloed design and operational approach across separate network domains was holding them back.[14]

Thanks to the open interfaces that intent-based networking controllers provide, NetOps teams will relinquish their isolated operational silo to become a fully integrated part of IT workflows. 34% of IT

leaders identified this change as the one that would most help the network team better meet the needs of the organization.[14]

However, in order to achieve the desired levels of IT agility and continuous intent alignment, NetOps teams will be charged with improving integration across network domains (access, WAN, data center, cloud, etc.) as well as with other IT domains, such as IT service management (ITSM) and SecOps systems.

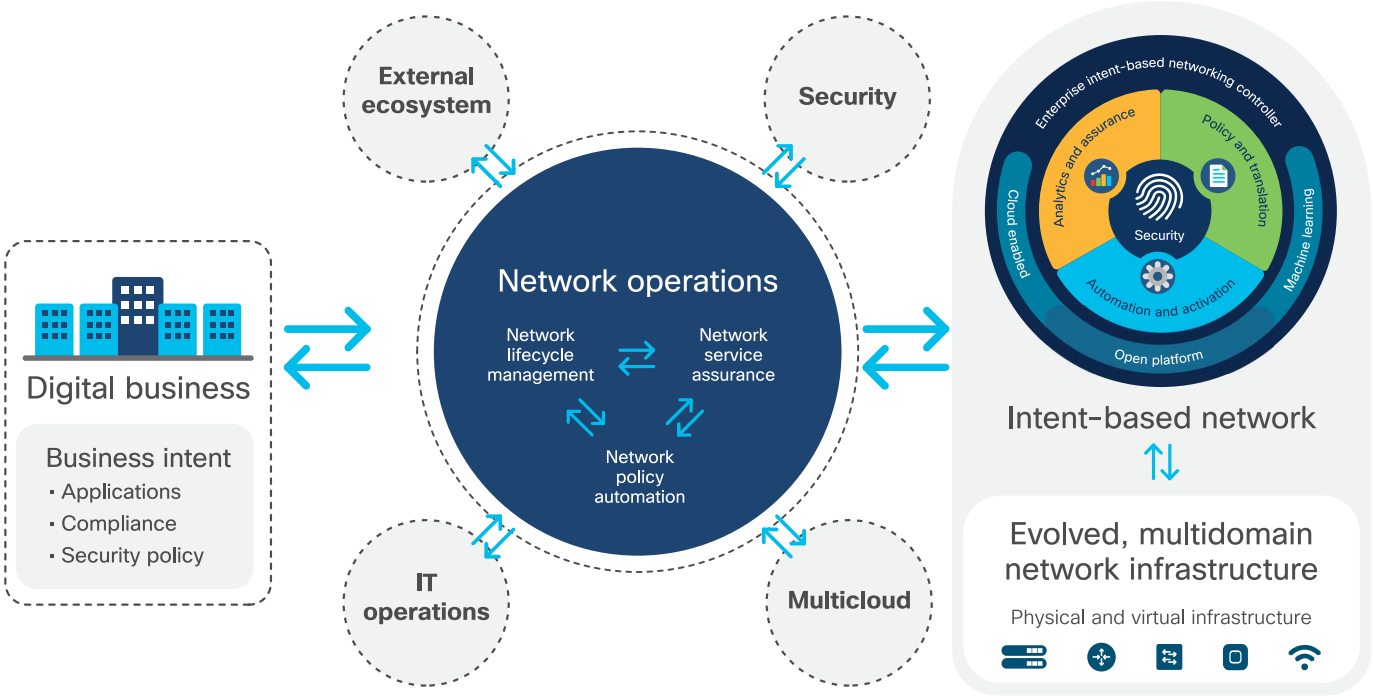
This figure illustrates how NetOps will be able to use an open-platform and network DevOps approach to integrate network technologies and processes with other internal and even external systems.

Full alignment with IT and business intent

In essence, the network exists to provide the services needed to support employees, customers, and partners—or in other words, to run the business. But the reality is that traditional manual-operations approaches often fall short of meeting dynamic business needs. That's about to change.

With intent-based networks, network operations will be much more automated and dynamic and will be directly informed by business and IT intent. Such intent would include application performance needs, security policy and compliance, and IT processes.

Figure 26 Integration opportunities with open-platform network DevOps approach



Over time, translation of business and IT intent into network policy will become an integral part of the network operations role.

Automation to reduce network operations complexity

There's no question that automation of operations tasks is changing the face of network operations. One-quarter of IT leaders and network strategists identified automation as the technology that would make the biggest impact on their network strategy and design over the next five years.[14]

However, this will mean leaving behind traditional manual approaches to configuring and maintaining the network. Some teams will find this unsettling, with 20% of IT leaders identifying reluctance among NetOps teams to adopt automation and AI technologies as a main obstacle to modernization.[14]

Preventive versus reactive problem and incident management

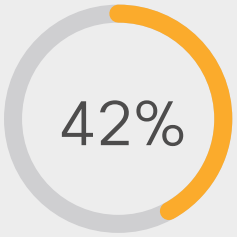
As discussed earlier, many organizations find themselves in a reactive stage of operational readiness. The challenge here is that 25% of respondents indicated that a reactive operational mindset was holding them back from achieving their networking objectives.[35] This, too, is about to change. By using AI and integrating with other IT systems, NetOps teams will be able to achieve a state of predictive maintenance that fixes problems long before they become incidents and impact services.

Human and artificial intelligence working in tandem

Network engineers need all the help they can get dealing with network complexity.

That's why NetOps teams are arming themselves with new AI-driven operations (AIOps) capabilities like machine learning and machine reasoning that can deliver more accurate performance baselining, anomaly detection, automated root cause analysis, remediation guidance, and predictive insights.

Instead of sifting through thousands of events, NetOps teams will increasingly rely on these technologies to accurately present only the most important ones, together with the top remediation options. The AIOps team may also work to fine-tune this output, enrich the content, and integrate the knowledge with key business and service management systems.



The move to AIOps is gathering momentum, as 42% of IT leaders believe that AI will have the biggest impact on their automated operations in the future.[35]

Bringing operational technology connectivity to network operations

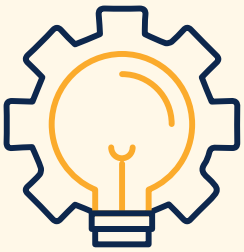
The fact that IoT devices are considered business assets, and that the operational data they produce is vital to business operations, clearly underscores the need for new approaches to infrastructure management.

- In IoT use cases such as real-time monitoring, operational problems could have serious, even life-threatening consequences.
- With large networks, IoT devices could number in the millions, so automation is the only way to manage them effectively.
- In some cases, there's no guarantee of a constant connection between HQ and remote IoT devices (which is driving investment in edge and fog analytics).

Introducing a next-generation network operations framework

To help prepare for a network operations future driven by intent-based networking, Cisco Customer Experience technology experts have created a framework that delivers strategic guidance, best practices, validated designs, proven processes, and recommended adjustments.

At the heart of this model are three critical process areas: lifecycle management, policy management, and assurance management. The operational simplification that IBN offers makes it possible to plan and build an operational transformation around these core processes.

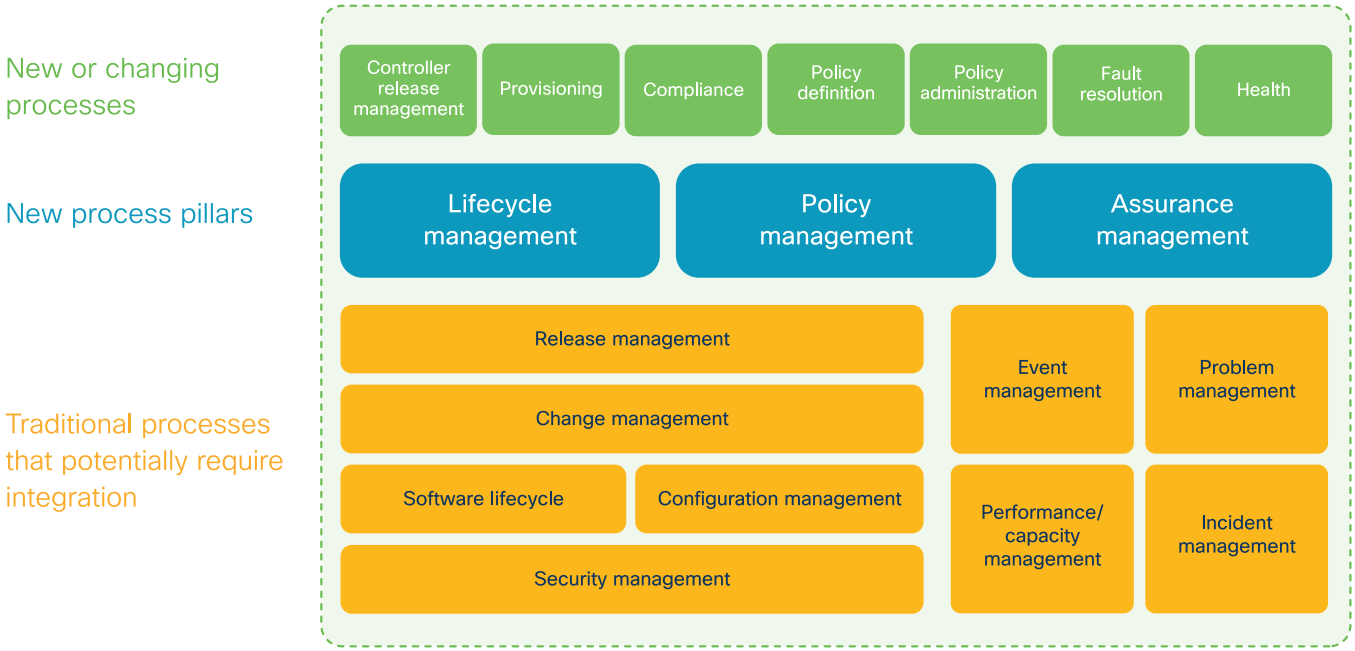


A new mind-set: Managing the network controller

According to Jake Hartinger, solutions architect with Cisco Customer Experience, one of the most profound changes in network operations will be the shift in focus from device to controller. Until now, network administrators have typically provisioned and collected information from the network by logging into devices.

With controller-based automation and assurance models, administrators will focus on managing the controller, the integrations, and the processes in relation to the controller. The more an organization is able to embrace this one change, the faster they will be able to improve service quality, cost, agility, and security.[36]

Figure 27 Emerging operations models for the new network



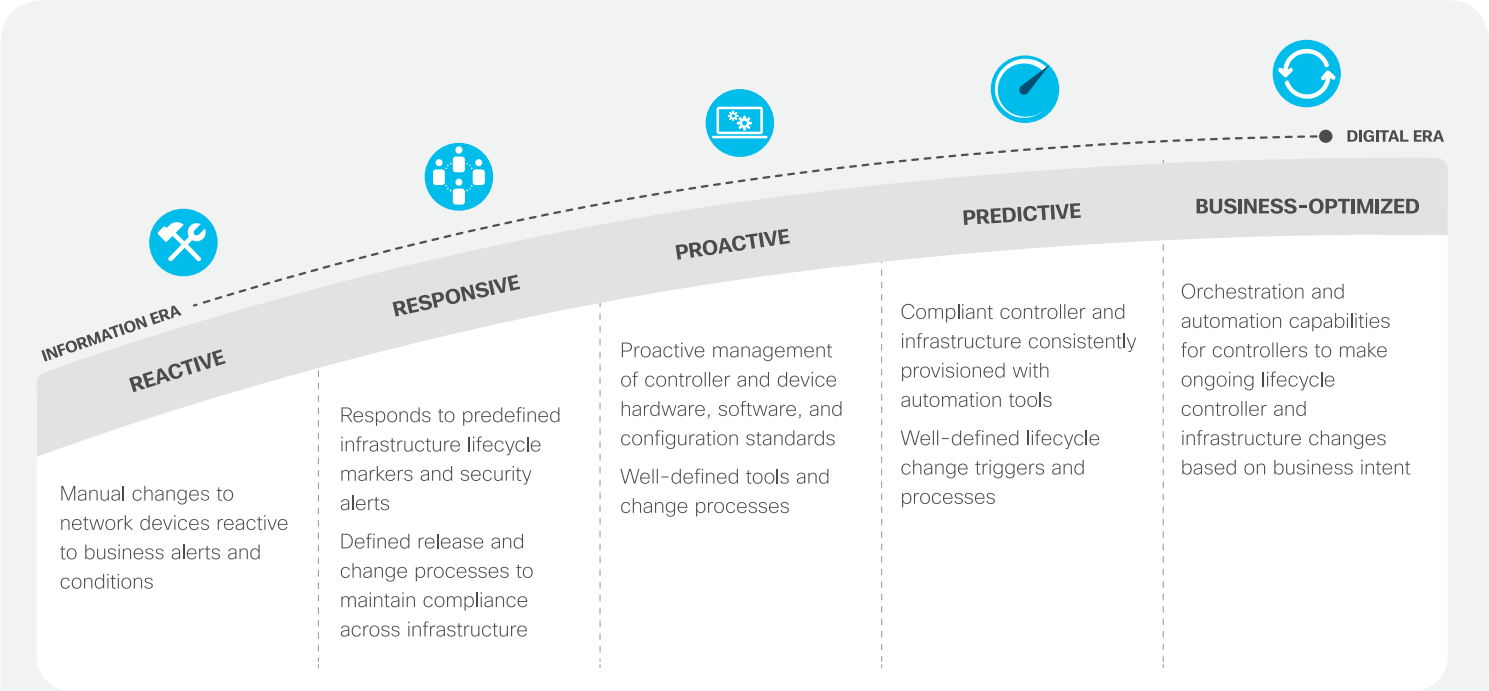
Lifecycle management

The change to controller-led automation and provisioning systems requires much stricter adherence to hardware, software, and security standards. A user making a command line interface (CLI) change may find that the controller will override the command in future updates because it is not defined as policy.

To avoid this scenario, the organization will need to have well-defined lifecycle management practices around release management and change management, especially with automations that focus on the network or service as a system.

Managing the network controller, in simple terms, involves managing new controller hardware, software, integration points and APIs, and the user-interface configuration that manages policy and assurance capabilities. Because controller capabilities will be continually changing for the foreseeable future, defining a unique lifecycle management process for the network controller and integrations will be paramount.

Figure 28 Network operations readiness: Lifecycle management

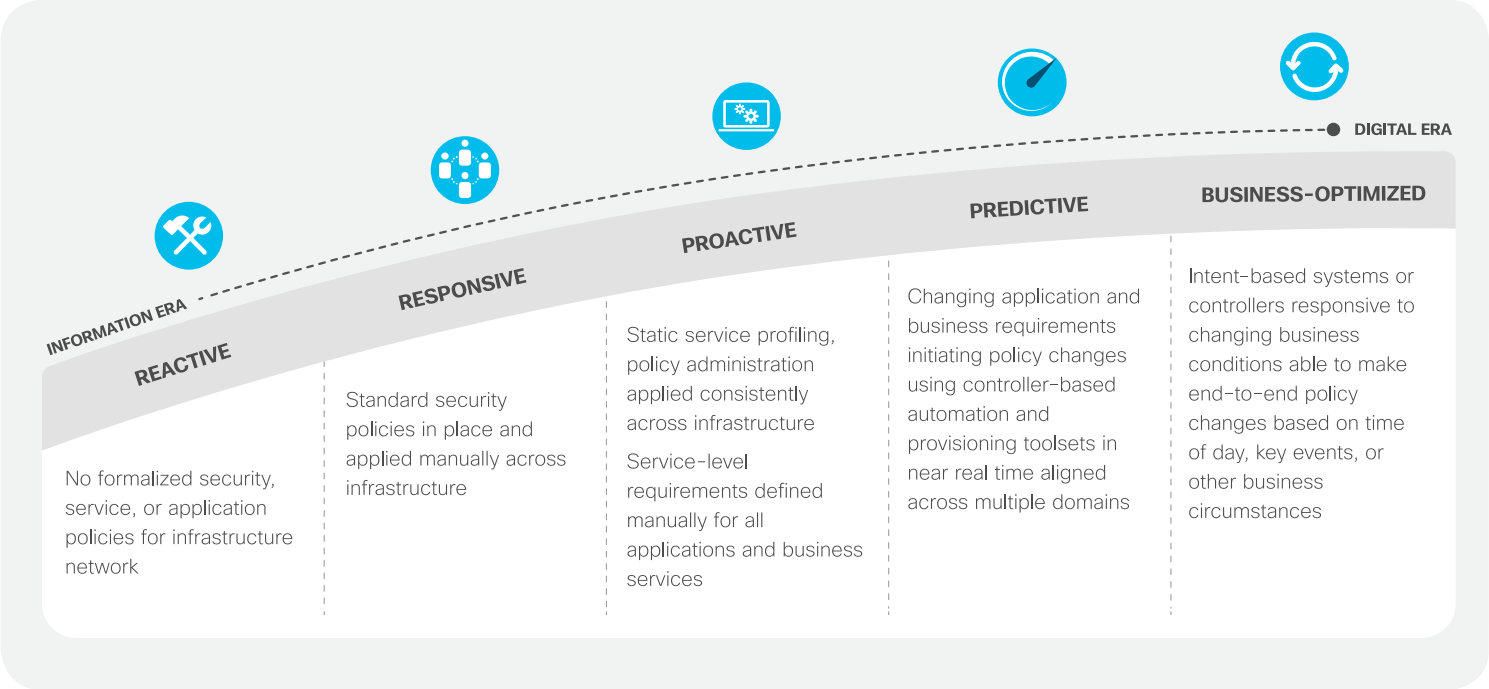


Policy management

Managing network policy is also essential because to be successful and sustainable, network controllers will rely on stricter network standards and guidelines for network device hardware, software, configurations, and even integrations. Policy must first be defined and then updated. It must also be configured within network controllers to ensure that defined standards are continually provisioned. Additionally, policy must be verified using compliance verification methods.

Because policy changes can have a very broad activation footprint, possibly affecting the configurations of thousands of devices, they need to be prescriptive in nature—so they can be tested and verified as valid and approved. Eventually, as model-based policy verification models that simulate any changes before they are activated become more widespread, there will be room for more flexibility in configuration options.

Figure 29 Network operations readiness: Policy management



Assurance management

Small networks tend to be easily managed with human hands and brains, but larger networks become nearly impossible to manage without tools, network data, and well-defined processes. Today only one in five operations teams have the ability to use advanced analytics to potentially identify and remedy service-impacting issues before they happen.[14]

With an AI-enabled intent-based networking model, assurance management improves and integrates these resources with analytics, API integrations, correlation capabilities, advanced inventory and reporting, and enrichment. In particular, analytics and enrichment provide additional details about network faults that facilitate rapid resolution or improved health. And with the expectation that the AI-enabled system will continue to improve based on learnings from large numbers of additional deployments, operations teams will continue to benefit.

In larger networks, the result is improved service quality, rapid issue resolution, and operational efficiency. An AIOps team might focus on filtering, enrichment, and APIs with business or service management systems to fully automate assurance workflows.

In addition to these three core process areas, we recommend looking at the possible interactions with traditional ITSM processes, IT domains, and systems to identify other potential integration opportunities.

Future of network operations predictions 2025

According to Rich Plane, CTO of Cisco Customer Experience, in five years' time, network operations teams are going to be much more effective at doing what their organizations need them to do. Here are his predictions on how this will happen.

1. **End-to-end assurance:** Network operations teams will be able to do predictive problem detection and root cause analysis between any client or device and any business service, hosted anywhere, and quickly pinpoint if and where the network is the cause of any service performance degradation.

2. **Bridging business and IT:** Network operations will be able to rebalance their focus from being almost exclusively engaged in monitoring and troubleshooting the network to also having an outward focus toward the business and how the network can best meet business needs. New operational roles will be chartered with understanding and translating business intent and application requirements into network policies.

3. **NetOps and SecOps operate from a single source of truth:** NetOps and SecOps teams will develop integrated and streamlined workflows enabled by data sharing, automated handoffs, and interactions between platforms and tools.

4. **NetOps extend monitoring to the cloud:** As multicloud business services become the norm, NetOps teams will extend visibility and predictive monitoring across WAN and public networks and to the cloud point of presence. For even greater insights, enterprise IBN systems will start integrating data from service provider and cloud provider systems to ensure continuous quality of experience for cloud services.

5. **Model-based change management:** More advanced NetOps processes such as "what-if" analyses of any changes being made on the network will extend beyond the data center and become more widespread.

6. **Self-driving, self-healing workflows:** Some less impactful workflows will be fully automated, allowing the network to take remedial or lifecycle management actions without human operator intervention. The result of this data-driven and intent-validated approach will be much higher levels of continuity of service due to minimized error opportunity.