Introduction

Unprecedented challenges, unrealistic expectations? Solving the most important network issues facing IT

Managing the IT skills gap. Protecting the business from a never-ending stream of sophisticated security threats. Ensuring IT and business alignment in a rapidly changing competitive climate, all while steering the focus away from routine operations and toward strategic innovation.

“The expectation about the art and possibility of technology use in business continues to be the CIO’s biggest challenge,” notes Bob Fecteau, senior vice president and CIO of Science Applications International Corp. (SAIC), a provider of government services and IT support. “There continue to be unrealistic expectations.”

There’s no question that today’s IT leaders face an unprecedented set of challenges, and many are embracing automation to streamline routine responsibilities. But beyond gaining efficiencies for day-to-day housekeeping tasks, there is a compelling case to be made for leveraging IT automation and, with it, a more sophisticated intent-based networking (IBN) model to address the larger issues surrounding IT modernization and digital transformation.

“The expectation about the art and possibility of technology use in business continues to be the CIO’s biggest challenge. There continue to be unrealistic expectations.”

BOB FECTEAU
SENIOR VICE PRESIDENT AND CIO
SCIENCE APPLICATIONS INTERNATIONAL CORP. (SAIC)
Taking the Pulse of IT leaders

Inhibitors to modernization

According to a recent IDG Quick Pulse survey, nearly one-third (30%) of responding IT organizations report being stretched too thin, but bigger-picture issues loom even larger. More than half (52%) of the survey participants are grappling with how to build up an IT talent bench with cutting-edge skills, especially in areas like software-defined networks (SDN), artificial intelligence (AI), machine learning (ML), and security, where pronounced shortages of seasoned experts exist.

Protecting the business from new global threats is top-of-mind for 42% of survey respondents—especially given the rapidly expanding attack surface as the Internet of Things (IoT), mobility, and cloud computing come on board and create new avenues for risk exposure. Also weighing heavily are concerns about improving IT/business alignment, with 32% of respondents aiming for greater agility and accelerating time to market as a way to retain their competitive edge.

Most Significant Pressures Facing IT/Network Team

- The need for IT Talent and emerging skillsets (52%)
- Protecting the business from new global threats (e.g., cybercrime, growing need for data protection & privacy) (42%)
- Rapidly changing competitive landscape (e.g., demand for greater agility and speed to market) (32%)
- IT/network staff are stretched too thin (competing priorities) (30%)
- Increasing cost pressures (26%)
- Explosion in data (e.g., volume and types — structured, unstructured) (24%)
- Always-on economy (e.g., same day delivery; 24x7 availability to the customer) (22%)
- Changing regulatory/compliance environment (e.g., GDPR) (22%)
- Empowered consumers/users (e.g., demand for seamless user experiences across all touch points and for real-time access to data) (12%

SOURCE: IDG Research 2018
**Automation provides relief**

Organizations such as SAIC are actively embracing advanced networking technologies and IT automation to address these and other pain points, but adoption is primarily directed to task-oriented activities, not big-picture IT challenges. For example, the IDG survey found that 66% of enterprises are automating threat detection, while 68% are completely or mostly automating performance monitoring. Automation is also expanding into areas such as network provisioning and orchestration (56%), policy configuration (54%), and issue resolution (50%). Day-to-day networking operations are the least likely to be automated, according to 48% of the respondents.

That said, survey participants do expect to advance the use of automation over the next two years, with the most significant ramp-up expected for issue resolution (jumping from 50% to 74%), policy configuration (54% to 74%), and network provisioning (56% to 76%).

Today, the bulk of IT/network automation is directed toward reducing risk (60% of respondents cited it as their first or second objective) and improving quality of service delivery (52%). Only 6% of respondents are currently considering network automation and intent-based networking as a means of achieving greater IT/business alignment and empowering new areas of innovation, while only 4% see potential in the technology to increase responsiveness to business needs.

Companies that successfully adopt intent-based networks have a better chance of aligning IT with key business objectives, resulting in better customer experiences, improved agility, and the freedom to redirect IT to focus on innovation and strategic business value.

“By embracing an intent-based model, organizations can respond dynamically to business needs and security threats while reducing the time they spend manually updating and configuring the network,” explains Prashanth Shenoy, vice president, enterprise networking and mobility, product marketing, at Cisco. “That enables them to apply freed-up resources to supporting more innovative infrastructure projects … that make the network a much more valuable asset to the business.”

---

**An Intent-Based Approach to IT Modernization**

Building on the concept of SDN, which largely automates the management of network infrastructure through programmability, the intent-based model is a closed-loop approach that tightly couples policy with intent to ensure greater flexibility and agility in response to rapidly changing objectives and the scale required for digital business. Based on open platforms, intent-based networking captures business intent in the language of business and translates it into IT policies that are automatically applied and continuously monitored across the network.

Intent-based networking encompasses three principal building blocks: translation capabilities for capturing intent, activation functions to automate the deployment of the expressed intent throughout the network infrastructure, and assurance to close the loop. This validates that the desired intent has been applied and outcomes have been achieved, including remediation and optimization through corrective actions.
Beyond automation: How an intent-based approach addresses the most urgent concerns of IT leaders

More than half of the IDG survey respondents (52%) believe intent-based networking can play a role in improving IT’s strategic position. Specifically, more than one-third (36%) said the closed-loop intent-based model can help IT align more effectively with dynamic business needs, and 34% are bullish on its potential to streamline operations workflow—both critical dynamics for freeing up IT resources to focus on more strategic initiatives and developing newly critical skill sets.

At the American Academy of Family Physicians, for example, the effort to modernize network infrastructure with automation and managed services has opened doors for some IT and network personnel to up their skills game and become more specialized, according to Michael Smith, vice president and CIO.

“Security and performance monitoring are key, but we have no desire to exponentially increase our staff in order to do that,” he explains. “By investing in the automation piece, we can reposition resources to focus more on [advanced] security capabilities without hiring additional people to do that.”

Survey respondents seemed to take a similar view: 22% view network automation/IBN as a tool to aid in talent acquisition by allowing employees to concentrate on higher-value projects, which in turn helps attract more skilled professionals, facilitates critical upskilling of the workforce, and aids in employee retention.
Responding to Survey Findings: A Roadmap to an Intent-Based Approach

Like the American Academy of Family Physicians’ Smith, the lion’s share (80%) perceive intent-based networks as a key component of IT modernization. However, while nearly all (94%) of the respondents to the IDG survey expressed an interest in developing an IBN strategy to achieve these and future goals, most are in the early stages of adoption and evaluation.

Organizations recognize they can’t simply flip a switch on intent-based networks and that they need to follow a measured approach to network automation and IBN. Enterprise Strategy Group Senior Analyst Bob Laliberte recommends the following action plan to help make the journey to intent-based networks smooth and successful:

**Develop an IBN roadmap.** Start with a digital network readiness model—an assessment of where an organization is on the network maturity curve—to provide a clear picture of priorities and next steps as they relate to core business needs and overall enterprise strategy. “Network projects are often prioritized and planned in response to the loudest squeaky wheel,” Cisco’s Shenoy says. “Because IBN requires a systems approach, it’s critical to have the destination in mind when starting any project. Whether your priorities are about improving security, accelerating application deployment, optimizing IoT initiatives, or about preventing downtime, they all advance you towards the intent-based goal.”

**Start small, but plan for an end-to-end architecture.** Map out an end-to-end architecture that transcends data center, campus, branch, the extended enterprise, and the cloud. At the same time, start implementing IBN components and processes in a single domain that correlates best to core business and digital transformation objectives. One of the easiest places to start is with network analytics and assurance. It’s estimated that more than one-third of network managers use 11 or more tools for monitoring and troubleshooting. Using an intent-based controller and analytics engine allows you to get a handle on problems even before they occur. Alternatively, with 80% to 95% of network changes being performed manually, another place to kick off the journey to intent-based networks is to automate repetitive administration tasks such as provisioning and configuration to reduce the management burden. Similarly, automating policy-based network segmentation can radically reduce the risk of attacks and address security headaches resulting from the growth of mobile users and IoT devices.
Embrace an open, standards-based model. The core value proposition of intent-based networks is for the system to configure resources to ensure that the needs of the business are continuously met. That means the network needs to be able to receive data from core business applications and be able to automate management of IT and non-IT systems across all domains (campus, branch, WAN, cloud, data center, etc.). As a result, intent-based networks require open interfaces to communicate and align policy and assurance across these domains and to successfully integrate into operational workflows. Addressed as an open platform, intent-based networks will ensure centralized visibility, management, analytics, security, and troubleshooting across multiple applications, systems, and heterogeneous network devices. An open platform will also ensure that your architecture has the flexibility to enable future use cases that have not yet been considered.

Prioritize security integration. Encourage collaboration between network and security teams to ensure that security is incorporated at every stage of IBN, across the “translation,” “activation,” and “assurance” functions. Of utmost importance: understanding what policies need to be in place so the appropriate levels of security are ensured and mapped to the application or set of services being deployed. “We have to be PCI compliant, our patient information requires that we address HIPAA, and GDPR is also important,” notes the American Academy of Family Physicians’ Smith. “Being able to utilize automation to exponentially manage multiple points of entry from a security perspective without increasing head count is critical.”

Factor AI and machine learning into the plan. As networks increasingly scale and become more dynamic and complex (especially in light of IoT and cloud computing), increased network intelligence is essential to help manage and ensure that prescribed service levels are being met from the data center to the enterprise edge. Integrated AI and ML capabilities will enable the analysis of vast amounts of data generated by networks worldwide and aid in insights that will trigger the appropriate action.

Identify trusted network vendors and partners. Given the complexity and scale of the journey, it’s important to align with partners who understand and can communicate the path to a full intent-based network architecture so everyone is on the same page. Create a checklist to evaluate vendors that incorporates key requirements, from open and standards-based architectures to a ground-up design for automation.

1 The Journey to Intent-Based Networking, Enterprise Strategy Group, By Bob Laliberte, January 2018
**Cultivate new skill sets.** It’s not just about the technology. The organization must cultivate the new skill sets, workflows, and organizational structures that will allow IBN to best support the business. Whenever possible, take the opportunity to develop internal personnel with new expertise in areas such as SDN, Python programming, RESTful APIs, and policy-based automation. Doing so will aid in employee retention and help narrow the ongoing skills gap both for newer technologies and for legacy network tasks, which won’t require the same number of IT resources with the advent of automation. “It’s increasingly difficult to find the numbers of network engineers today to support the growing demands and scale of the network,” Cisco’s Shenoy says. “Now you’re able to take people and make them more efficient and effective in supporting the business by adding skills to their repertoire and by automating the way they provision and maintain the network.”

**Conclusion**

There is so much promise for network automation and intent-based technology beyond facilitating mundane IT housekeeping tasks. Armed with an open set of technologies and the right partnerships, IT organizations can ride the wave of automation and IBN to take on some of their most pressing challenges and elevate IT’s role in strategic business transformation.

To learn more, go to [www.cisco.com/go/IBN](http://www.cisco.com/go/IBN)