www.pipelinepub.com
Volume 20, Issue 6

Minimizing Network Downtime in the Age of Digital Transformation

By: Gary Marks

In the digital transformation era, businesses across all industries rely increasingly on the network. Maintaining an "always-on" network is crucial to ensuring the effectiveness of this era's various technologies. Whether it be robotics and the Internet of Things (IoT) or advanced analytics and cloud solutions, these technologies rely on a consistent network connection to remain operational. One disruption could grind essential operations to a devastating and costly halt, causing significant damage to brand reputation and business relationships.

The transformative shift toward automation through generative artificial intelligence (Gen AI) and machine learning (ML), and the processes they enable, would not be possible without continuous network uptime. Should a network outage occur, automated Gen AI-powered chatbots, for example, could not interface with customers to collect payments, answer questions, etc. Likewise, remote work, which requires digital tools for communication and collaboration purposes, can become compromised if the network falters.

Put simply, network downtime is one of the greatest threats to efficiency, success, and prosperity for any business engaged in digital transformation. Unfortunately, but perhaps unsurprisingly, 96 percent of U.S. businesses experience at least one outage quarterly. As this article will later discuss, digital transformation is one of the primary drivers for this increased frequency of network outages. To that end, it is of the utmost importance that enterprises build a more resilient and robust network capable of enduring disruptions to normal operations, thereby safeguarding digital transformation efforts.

Why Digital Transformation Increases the Risks of Network Downtime

The technologies and innovations brought on by digital transformation support unprecedented performance, flexibility, and productivity. Other benefits of digital transformation include improved decision-making, profitability, and sustainability, as well as enhanced connectivity between information technology (IT) and operational technology systems. Nevertheless, this rapid increase in complexity places an enormous strain on the network, skyrocketing the risk of disruption and downtime.

Simultaneously, digital transformation widens the attack surface, increasing the likelihood of network outages. The highly interconnected nature of enterprises (especially those that employ thousands of IoT devices) opens new pathways for bad actors to slip undetected into an enterprise's digital environment. Once inside, they can manipulate control systems, steal sensitive information, and access critical network applications. Complex software stacks, for instance, need routine updates, where they are temporarily vulnerable to bugs, exploits, and cyberattacks. Remote workforces also present new security challenges for businesses and exploitation opportunities for bad actors. Internal or external, these threats often have a domino effect, creating prolonged network downtime.

Other factors that might trigger network downtime include, but aren't limited to, Internet service provider issues, fiber cuts, and human error. Unplanned maintenance can also force businesses to shut down the network temporarily. Additionally, naturally occurring events, such as severe weather or natural disasters, while rarer, can jeopardize network uptime.

The Consequences of Network Downtime

The consequences of network downtime can be severe and far-reaching. Perhaps the most obvious effect of a disruption is the cost, which, for an average business, is $4,344 per minute. And considering an average outage lasts at least five minutes, those businesses, at minimum, are taking a $21,720 hit every time an outage occurs. Furthermore, enterprises can get behind schedule if the network and all the digital technologies it powers stop functioning. Likewise, consumers can't access online services, degrading customer experience and damaging brand reputation. A company notorious for network outages is less likely to retain and attract customers or maintain partnerships, further impacting its bottom line.

Worst of all, downtime may impede digital transformation efforts, as IT personnel and technicians are constantly putting out fires rather than focusing on innovation. In many cases, network engineers must also travel on-site to physically remediate issues and restore operations, which can be an arduous and time-consuming process. Other non-technical employees within the organization are impacted similarly by downtime. Most workers need a stable network connection to perform their jobs. Even clocking in may be impossible during downtime. This ordeal is stressful for everyone, reducing staff morale and productivity while potentially increasing turnover.

What is Out-of-Band Management?

Enterprises need a network solution to minimize downtime, maintain operations in the face of faults and safeguard digital transformation. One leading approach that businesses should use to foster a more resilient network is out-of-band management. Many enterprises use in-band management, which uses the network itself as a media to manage devices through common protocols, like ssh and https or Secure Shell. Although in-band management is cheaper and simpler than out-of-band management, it is not secure. Moreover, the most problematic aspect of this method is that during network disruptions, a company's technicians become locked out of the primary network and are thus unable to remediate issues.

However, unlike in-band management, out-of-band management separates and containerizes the functions of the management plane from the data and control plane. Effectively, out-of-band management allows a district network (also known as the out-of-band network) to operate independently from the primary in-band network. Even if the primary network goes down, this separate layer permits network engineers to detect issues, access critical applications, and restore operations quickly, securely, and remotely. Most importantly, out-of-band management enables enterprises to build a robust network that can recover swiftly from network outages while upholding an appropriate level of service amid various disruptions, be they cyberattacks, human error, etc.

Safeguarding Digital Transformation with Out-of-Band Management

By utilizing out-of-band management, businesses can ensure that digital transformation remains undisturbed even if the primary network experiences disruptions. This resilient network allows employees to continue to leverage solutions, such as Gen AI tools and advanced analytics, that require network access. Likewise, there won't be gaps in data. For example, IoT devices and sensors that help monitor the status and output of factory machines will continue functioning. In the same way, customers shouldn't notice a considerable drop in quality of service, whether accessing their profiles or using online services, maintaining revenue generation and preserving a seamless customer experience.

Leading out-of-band management technology also allows enterprises to more effectively repel and fight against those cyberattacks brought on by the expanded attack surface of digital transformation. Should malware or ransomware cause a breach, engineers can use the out-of-band network, an independent management plane, to lock down critical functions on the production network. At the same time, they can continue to configure and manage devices on the out-of-band network. This technology also enables engineers to shut down servers and disconnect wide area network connections, further isolating a breach to only impacted network equipment. Engineers can even leverage out-of-band management to restrict access to critical devices and functions, permitting only authorized personnel and preventing internal bad actors or unaware employees from tampering.

Out-of-band management will further support digital transformation strategies by accelerating network processes. For example, out-of-band management empowers engineers to streamline configurations and day-one provisioning, helping to get remote sites up and running quickly and at scale. It also simplifies other everyday tasks like IT infrastructure management and monitoring. Moreover, because engineers can monitor, manage, and remediate network devices remotely, they don't have to travel on-site to troubleshoot issues; instead, they can focus their energy and resources on digital-first initiatives, ultimately helping businesses stay competitive.

In the same vein, the ability to access and manage critical network infrastructure from anywhere through out-of-band technology opens the door to remote and hybrid work models. Digital transformation made remote work feasible for many employees. Now, out-of-band management makes remote work possible for most, if not all network engineers, administrators, and technicians. Again, if there is a network disruption, these technical employees don't need to drop whatever they're working on and drive to some far-flung location. As such, out-of-band management serves as a valuable recruiting differentiator, helping enterprises attract the best available talent and extend their geographical reach.

Coupling Digital Transformation with Out-of-Band

Digital transformation is inevitable. In fact, research shows that 93 percent of all companies have already adopted a digital-first business strategy or have plans to adopt such a strategy. As demonstrated in this article, one of the unintended consequences of digital transformation is the increased risk of network downtime. Accordingly, there needs to be a mindset shift among companies where digital-first strategies and initiatives coincide with the simultaneous implementation of network solutions like out-of-band management.