www.pipelinepub.com
Volume 17, Issue 1

End-to-end Resilience for the Evolving Network

By: Simon Pincus

There's a plausible future we can all envision. Consumers everywhere will be looking for unnoticeable latency and instant gratification as they work remotely, stream their favorite shows via higher resolution formats, or access immersive experiences through mediums like AR and VR. And all around, there will be a buzz of data-intensive IoT technology at work, such as self-driving vehicles, smart city infrastructure and sophisticated AI-driven devices. All of this will be powered by edge infrastructure, including remote offices and cell towers, and a rise in 5G to handle the traffic.

This view, which seems straight out of a sci-fi novel, may not be so far off. Statista projects that global spending on smart city projects will reach over $1 trillion by 2024, while IDC predicts that in 2025 IoT devices across the globe will create over 90 zettabytes of data. Grand View Research predicts the edge computing market will be worth $43.4 billion by 2027. While these advancements paint a very intriguing, cutting-edge picture, it's crucial to examine what it all means for the backbone that will support it all: the network infrastructure.

Put simply, ensuring near zero latency, optimized quality of service and minimal disruptions will become more challenging and vital than it has ever been. We are already seeing this play out now via the combined impact of users demanding high reliability, network complexity growing alongside new edge deployments, and increasingly frequent disruptive events, like weather storms, protests and public health crises.

As technology evolves, networks will still need to withstand forces that can cause disruptions. This means that network resilience—the ability to supply and maintain optimal service levels under all conditions—is something every enterprise should consider as they seek to maintain connectivity for the increasingly distributed, data-intensive networks of today and tomorrow.

A future with increased points of failure

There are many factors that can lead to network downtime, and every remote network node introduces new points of failure. These points could fail and disrupt service via issues like last-mile power cuts, bad software updates, unseen security breaches and simple human errors. Additionally, edge sites may be harder to reach, and other technologies, like SD-WAN routers, can introduce even more points of failure via software stacks that are prone to breaches and bugs. As one can imagine, if networks adopt more IoT and edge infrastructure to support it, organizations will need to make sure they are prepared to handle the additional vulnerabilities from added network nodes.

The costs of downtime

While the future may bring more points of failure, the costs of network disruptions are already severe. In fact, Opengear recently polled more than 500 senior IT decision-makers worldwide and found that network outages cost more than one million dollars annually for nearly two-fifths of US businesses. The study also found that the top impacts of outages were decreased customer satisfaction (41 percent), data loss (34 percent) and financial loss (31 percent).

This research suggests that it is important to both prevent disruptions and to have procedures in place to quickly recover from them. Such precautions will go a long way toward keeping operations moving and customers satisfied.

As one can imagine, the more connected we become, the more likely it is that the costs of network disruption will skyrocket while the benefits of an ironclad network infrastructure may go up as well. Following are some practices every organization can follow to ensure network resilience now and in the future.

Separate network management

The primary production network is accessed by a large pool of users. This makes it more vulnerable to cyber breaches and disruptions, and if network management is housed on the same network, it becomes susceptible to the production network's issues. This means organizations may be wide open to attacks from anyone who can connect to a vulnerable device, and management can get locked out during disruptions and cyber-attacks. A Twitter link could open the door for data theft, or a bad update could lock out management from quickly resolving an issue.

Providing a separate, or out-of-band, pathway for network management to connect to edge and core console ports can prevent deadlock, drastically secure the "keys to the kingdom" of an organization and provide a secure "admin's only" location for network management resources.

With a separate network management plane, automated tools and technicians can constantly monitor equipment and remediate problems, regardless of the primary network's status or the location of the incident. It can also help management carefully gate access to many features for improved provisioning and new site configuration. This could be immensely helpful to maintaining always-on connectivity for consumers and enterprise users alike.

Develop a network management automation toolset

While automation reduces the workload burden of skilled technologists, it can also increase security for critical network devices. For instance, automated management tools can constantly log, analyze, and generate alerts based on network activity. Modern tools can also continuously update critical resources like back-up images or firmware update scripts. Additionally, capabilities like zero-touch provisioning can make new site configuration remote, instantaneous, and secure.

Many are familiar with the idea that ongoing updates can drastically prolong the life of certain software. Applying this concept to networking, many organizations seek to develop ecosystems that prepare them to continuously improve upon and update their network management tools and automated networking functions. This can help them ensure their networking environment aligns with their overall architecture and business strategies, which may be shifting, and ensures agility for years to come.

For easy updating of network automation tools, open-source solutions are often key. To this point, organizations have drastically improved their flexibility and scalability by implementing open-architecture models. These can act as a secure, network-management staging ground conducive to third-party tools and in-house automation modules alike.

Implementing secure wireless connectivity

Many find that a backup connection should be able to seamlessly prevent disruptions and scale alongside an organization. For those looking to future-proof, plain old telephone lines are probably not ideal because they are difficult to scale. Additionally, they are a poor backup solution because they are vulnerable to the same disruptions as the underlying network. Telephone lines are also inefficient for servicing geographically dispersed edge locations because they need on-site support for troubleshooting and configuration.

As opposed to phone lines, a wireless cellular connection can provide organizations with reliable and scalable link diversity for failover and new site set-ups that can be performed remotely. As part of a failover solution, cellular connections can provide enough bandwidth to allow critical functions to continue to operate as the network is restored.

When configuring a backup cell network, companies can also benefit from automatic failover capabilities as well as security protocols that can gate traffic and increase device visibility. These security features can ensure the back-up solution is not used by hackers to access the business system.

It is important to note here that initial 5G rollouts could depend on costly supporting infrastructure, so its implementation may be restricted to higher-bandwidth use cases. For network management, LTE networks could remain more feasible for several more years. This is because network management does not need to handle large quantities of user data. Therefore, LTE may work as a cost-effective backup line for the management plane as 5G adoption gains ground.

Ensure data-rich applications are supported at the edge

IDC predicts that almost 30 percent of the data used in our personal and business lives will be processed in real-time, while New Vantage Partners' data indicates 97.2 percent of executives are investing in Big Data and AI initiatives. When you combine these findings with trends towards increased edge computing to support IoT and other data rich processes, it places a plethora of sophisticated devices at various remote sites.

Much more than carrying out simple tasks like reading temperatures in a data center, the new breed of edge devices will likely need to respond in real-time for mission critical objectives like managing self-driving vehicles or using AI to sort through massive amounts of information to find the right data to be taken back to the core infrastructure for further analysis.

The edge computing infrastructure required to support data-intensive processes locally will likely need to feature streamlined, always-on methods of monitoring, provisioning, and remediation to provide resilience. This means, more than ever before, technicians and management tools will need to operate in sync and have a remote connection to every and all devices. And though networks may experience issues, the less the user feels these problems, the better it will be.

There's no time like the present to future-proof

As consumers depend more on their virtual worlds and digital devices, and our everyday tools become increasingly connected, network complexity will undoubtedly grow at the core and edge. Enterprises and Internet service providers alike will need to ensure their network infrastructures are robust enough to deliver the seamless quality of services that users demand.

For a seamless user experience, network resilience could be the most important component to consider, and an end-to-end approach to this is all about ensuring all devices in geographically dispersed areas are backed by solutions to monitor all networking equipment, prevent system disruptions and rapidly recover from outages. In this regard, it may benefit many to start preparing for the massive connectivity of tomorrow today, before problems necessitate change.