SMART NETWORK RESILIENCE

DEREK WATKINS, VICE PRESIDENT OF SALES EMEA & INDIA AT OPENGEAR MAKES THE CASE FOR OUT-OF-BAND NETWORK ACCESS AS A SUBSTANTIAL AID FOR CREATING THE HIGHEST LEVELS OF NETWORK RESILIENCE

It's clear with the plethora of growing trends including cloud, SaaS and mobility, that the edge of the network is becoming more diverse, complex and harder to define and manage. Yet the fundamental requirements still build around reliability and uptime. To deliver the high levels of resilience expected many organisations are endeavouring to extend the troubleshooting reach of centralised NOCs and automate more network administration tasks in an attempt to achieve this.

As the criticality of IT systems has increased, the corresponding cost of unexpected outages has also risen and never fails to surprise. Earlier this year, analyst firm Infonetics Research conducted in-depth surveys with 205 medium and large businesses in North America and discovered that companies are losing as much as $100 million per year to downtime that is related to information and communication technology. A closer analysis of the root causes conducted by the Ponemon Institute found that the IT equipment failure followed closely by human error were the two major causes. In response to this, organisations are increasingly investing in technology and evolving processes to improve network resiliency by directly addressing these two pressure points.

Although network elements such as switches, routers and firewalls have steadily improved in reliability, some hardware failures are of course inevitable. In the best case failure, a network element will fail cleanly allowing redundant equivalents or active elements to seamlessly take over its tasks. Unfortunately however, failure is not uniform.

The worst case scenario is a transitory or intermittent fault which impacts performance but fails to initiate failover. In this case, IT teams need to be able to quickly initiate troubleshooting tasks such as hard-reset, power cycle or configuration changes. This is where Smart out-of-band (Smart-OOB) connectivity can effectively extend the reach of the system administrator to access devices, which in some cases cannot be reached by the disrupted production IP environment.

Smart-OOB provides an alternative path to connect with the internal console of remote devices, including a failover to cellular 3G/4G or Wi-Fi connectivity and in turn facilitates those vital management tasks remotely. Such a smart appliance can also connect to power distribution units (PDUs) to initiate power-cycling on connected equipment, often an effective method of fixing some issues in the event of an unresponsive device.

The other area where Smart-OOB can help improve resiliency is in mitigating the impact of human error. In a typical installation, the Smart-OOB appliance sits in the command path between network administrators and individual devices: it acts as a gatekeeper during tasks such as configuration changes and firmware updates. This enables the appliance to maintain a continuous audit of changes to allow for rapid roll-back to previous configurations in the event of a problem. This audit logging and alert function also enhances operational security by making malicious changes more difficult to carry out undetected.

The final aspect is fault detection and automation. Unlike traditional network management tools which tend to poll devices over production IP networks, a Smart-OOB is directly connected to each device within the rack and it is able to gather more granular real-time data with alerts based on a wider set of criteria. For example, with the appropriate sensors installed, a Smart-OOB device could generate alerts for temperature thresholds, humidity warnings, UPS battery failure or even physical tampering if a rack is opened.

As organisations continue the transition to diverse network infrastructure, the need for resiliency in production, support, and management remains paramount. By using a Smart-OOB tool, IT teams can deploy an intelligent, reliable means to detect issues before they escalate operationally affecting users, and quickly remediate problems even if the production IP network is down. NC