RESOLVING NETWORK ISSUES WITH THE RIGHT TOOLS LIES AT THE HEART OF OPTIMAL NETWORK PERFORMANCE. LUCKILY, TECHNOLOGICAL ADVANCES IN NETWORKING MONITORING, TESTING AND TROUBLESHOOTING MAKES THIS TASK THAT MUCH EASIER FOR NETWORK MANAGERS.

Networks face a myriad of issues many of which can go unnoticed for ages before delivering a potential devastating blow to the network.

A recent survey of 3,000 network professionals by Fluke Networks, global provider of cable testing equipment for LAN networks, test sets and other network troubleshooting & performance management solutions, found that 82% of respondents ranked network and application performance problems as a concern or critical issue, with 52% stating that a Network Management Station (NMS) has insufficient capabilities to get to the root cause of the problem most or all of the time. 51% of respondents said that they needed to leave their desk some or most of the time to troubleshoot the problem.

Nagging, intermittent problems can 'hide' in the network, reducing both productivity and the credibility of the IT department, observes Ramesh Reddy, solutions manager, MEA & Turkey, Fluke Networks, "To investigate and resolve performance issues quickly, the engineer needs end-to-end visibility across the network: a dedicated solution for automated network and application analysis that fills the gap between traditional NMS and packet capture," Reddy says.

According to Dev Anand, director, Product Management at ManageEngine, delivering business critical apps at promised speeds and SLAs is the biggest challenge for any network team. However, Anand adds, bandwidth issues, network health, configuration management, and security threats are some other major issues that disrupt the service delivery.

Taj ElKhayat, regional VP, Middle East, Turkey, North, West, and Central Africa at Riverbed Technology, says one of the major trends affecting networks is the advent of the hybrid enterprise. "Today, IT must provide an environment where users can access applications, data, and the underlying infrastructure located on-premises in data centres and private clouds and consumed as services from public clouds. Such a consumption model is what Riverbed Technology refers to as the 'hybrid enterprise," ElKhayat says.

A hybrid IT environment by its very nature is more complex than either a pure on-premises or cloud-based business, ElKhayat explains. "In the hybrid enterprise, people, apps, and data are everywhere. IT departments must accommodate for employees who now work from multiple locations, and must handle corporate data that lies outside their data centres. Going hybrid adds architectural complexity and blind spots for support, management, and security. The challenge for CIOs in the hybrid enterprise is to gain visibility and control of all resources – those shared in public clouds and those managed on-premises across a highly distributed enterprise," ElKhayat says.

eHosting DataFort's director of operations, Tamer Saleh, on the other hand identifies the main issues affecting networks as performance degradation where loss of speed and data integrity occurs due to poor transmissions. This is in addition to security issues that involves maintaining network integrity, preventing unauthorised users from infiltrating the system and protecting the network denial of service attacks.

With almost all organisations, big and small, now dependent on their networks for day to day business operations, effects of network flaws run the whole gamut of industries and segments.

ElKhayat contends that all organisations are susceptible, but it is often the largest enterprise organisations that have the most at stake. "The distributed hybrid nature of their networks means there a large number of potential points of failure. These organisations also have distributed employee and customer bases that served by web-based and even mobile applications. When network bottlenecks occur and these applications fail to perform, it directly impacts productivity as well as the brand image," ElKhayat says.

Saleh concurs, saying organisations with larger networks are more susceptible to network issues including attacks as they have more points through which their network could get compromised. "More staff also means more devices and passwords and a greater chance to get attacked as employees are the weakest link in an organisation's security policy," says Saleh, adding, "In addition, over the years we have noticed that organisations with valuable data are most susceptible to targeted network attacks."

Reddy attributes these problems with networks due to the fact that the vast majority of organisations do not follow a standardised troubleshooting process. Not only does this process vary within an organisation but the tools used to troubleshoot problems vary substantially, Reddy observes.

According to Reddy, technicians can't resolve the problem

> "Problems may result from a proliferation of Wi-Fi devices, excessive use of bandwidth by unauthorised applications, configuration errors, poor application delivery infrastructure or many other sources."
>
> **Ramesh Reddy, solutions manager, MEA & Turkey, Fluke Networks.**

Reddy observes that technicians may not resolve the problem themselves in many cases and may need additional help with difficult problems.

themselves in many cases. Sometimes they need additional help with especially difficult problems. In other instances, it's because the problem lies outside their domain of responsibility, and they need to work with a separate group inside (server management or application developers) or outside the enterprise (service providers or equipment vendors).

With the network so crucial to business operations, investing in a proper network monitoring, testing and troubleshooting strategy is crucial.

Reddy notes that with the network such a strategic asset to the business, any downtime or degradation in network or application performance will directly impact the organisation's bottom line. "To deliver the service levels agreed with the business, the challenge is two-fold: proactively improve and optimise performance to ensure that the network delivers what users require, and resolve any problems that arise as quickly as possible to minimise downtime," Reddy adds.

Getting to the root cause of network and application issues is increasingly difficult and time-consuming in today's enterprise networks, Reddy acknowledges, with virtualisation extending from the data centre to the desktop while the growing popularity of cloud services and BYOD reflect shifting work patterns and cultural change.

"Problems may result from a proliferation of Wi-Fi devices, excessive use of bandwidth by unauthorised applications, configuration errors, poor application delivery infrastructure or many other sources. The increasing inclusion of voice and video adds more complexity and pushes bandwidth to its limits," says Reddy, adding, "Solving performance problems is made more difficult and time-consuming by the challenge of trying to ascertain whose responsibility they are, particularly when all groups are reporting green KPIs."

Network monitoring and troubleshooting go hand in hand, Anand says. Monitoring allows organisations to be proactive and identify faults and issues at the very early stages. This helps them to troubleshoot before the faults/issues get big and pose a threat to business. "Testing helps organisations identify the maximum load their networks can handle. It helps them simulate traffic and find out how much they can scale and how many users they can support, and plan accordingly for future expansion," Anand adds.

As vital as it is for companies to invest in network monitoring, testing and troubleshooting, doing so in-house can be expensive, stressful and time-consuming, Saleh argues. "Today, organisations are finding it increasingly challenging to hire, train and retain IT personnel with specific skill sets across various domains. Therefore, many companies are opting for a more reliable alternative – partnering with an IT services provider to remotely monitor and manage their networks and IT systems."

Remote monitoring and management (RMM) services thus offer proactive solutions to manage networks, devices, users, desktops and data, ensuring efficient, highly available and completely supported IT infrastructure, Saleh explains. Benefits of RMM services are many and include efficient, highly

> "Today, organisations are finding it increasingly challenging to hire, train and retain IT personnel with specific skill sets across various domains."
>
> **Tamer Saleh, director of operations eHosting DataFort.**

ElKhayat says trying to troubleshoot performance and availability issues in the cloud is tricky.

Saleh says many companies are partnering with IT service providers to remotely monitor and manage their networks and IT systems.

Anand advises a problem once identified be eliminated at the root level so that it doesn't arise again.

> "Testing helps organisations identify the maximum load their networks can handle and also simulate traffic, finding out how much they can scale and how many users they can support, therefore plan accordingly for future expansion."
>
> **Dev Anand, director, Product Management, ManageEngine.**

available and completely supported IT infrastructure, time saving, overall increase in the efficiency of networks, reduced hassles of IT complexities, enhanced security as systems are monitored 24/7 for security threats and hacking breaches, among other advantages.

A typical testing and troubleshooting procedure depends on the situation at hand, experts contend.

Riverbed recently undertook a survey by interviewing 20 customers to understand their procedure for diagnosing a typical network problem, ElKhayat reveals. According to the report, 19 out of the 20 customers always started by looking at the same basic network information before deciding on an approach. This information includes: utilisation, top hosts, top interfaces, top ports, top apps, QOS markings, etc. The procedure from there on varies depending on what the problem might be, ElKhayat says.

The next step is inevitably, rectifying any issues discovered.

A problem once identified, Anand says, has to be eliminated at the root level so that it doesn't arise again. "The next step would be to automate the troubleshooting steps so that even if the problem does recur, it doesn't need any manual intervention," Anand advises.

Reddy recommends a series of steps as best practices to follow after a problem has been detected. These include Identify the exact issue or problem, recreating the problem if possible, localising and isolating the cause and then formulating a plan for solving the problem.

After this, Reddy says, IT should strive to implement the plan, test to verify that the problem has been resolved, document the problem and solution and finally provide feedback to the user to encourage them to report similar situations in the future, which will improve the performance of your network.

Anand, of ManageEngine, says the majority of the network management activities are the same for most of the organisations and don't require much customisation. "In turn, most vendors don't ship solutions that have been customised specifically for individual organisations or industry verticals. Rather, they provide options that are customisable as per the organisation needs," he adds.

Cloud is becoming major trend in testing and monitoring industry, like elsewhere.

That said, SaaS applications do create new challenges for the industry. "To effectively troubleshoot performance and availability issues in the cloud is a thorny issue," argues ElKhayat. "As the level of complexity continues to grow, enterprise IT must invest in solutions, which allow them to achieve the same level of control and visibility for all connections, whether they originate from the data centre, the branch, a mobile device or a SaaS application."

Challenges in the industry take the form of limitations of the diagnostic tools themselves.

"IT support teams are typically siloed using their tool of choice but this presents a challenge in that these disparate toolsets provide no correlated view into performance issues that may be present within any component across the application delivery infrastructure. Without the ability to understand how one component may affect another at a specific point in time, it becomes difficult if not impossible to quickly understand how well the infrastructure is transporting applications, how well those applications are performing, and where the problem truly lies," says Reddy of Fluke Networks.

Typical tools offered in the industry are based on SNMP polling mechanisms, which provide visibility into network problems, but cannot show service/business priority. Other tools require extensive configuration into the product to bring visibility into network problems. Both limit how enterprises can manage their borderless enterprises.

"This is where Fluke Networks with its wired and wireless portfolio for application & networks performance monitoring brings a unified visibility across the organisation," says Reddy. "Fluke differentiates with unique features like few clicks to problem resolution, focus on end-user experience while giving power to IT to connect end user response times to problem identification and isolation," he adds.