Strategies for network optimisation

As UK organisations face soaring digital demands, network optimisation has shifted from a technical challenge to a business imperative. This feature explores how scalable design, intelligent tools, and airtight security can future-proof IT infrastructures…

Optimising IT networks in the UK isn't just about speed — it's about building infrastructures that can adapt, self-heal, and scale in line with ever-growing demands.

"Comprehensive network planning starts with understanding how people and devices interact with the environment," says Gerard Donohue, Chief Technology Officer at Telent. "By analysing data from connected systems like sensors, cameras, and endpoints, it's possible to predict where bottlenecks are likely to emerge and plan accordingly."

Hamzah Malik, Solutions Consultant, CACI, agrees, stressing that modular, hierarchical design is key to scalability: "comprehensive planning and scalable design are the foundation of a future-proof network. Modular architectures allow organisations to scale capacity without re-architecting the entire infrastructure. With tools like network modelling, capacity planning, and SDN, businesses can anticipate demand and flex bandwidth as needed."

Together, these strategies mean organisations can scale intelligently — avoiding costly redesigns and ensuring networks grow as fast as their businesses.

Why cutting corners on equipment costs more

Cheap hardware may seem like a bargain, but it can cripple performance and security in the long run. Investing wisely is key.

"Enterprise-grade equipment from trusted vendors like Cisco, Juniper, and Fortinet undergoes rigorous testing, offers advanced telemetry, and benefits from ongoing software support. This investment translates to greater stability, better visibility, and improved automation capabilities, which ultimately lowers operational costs over time. Cutting corners often leads to downtime, vulnerabilities, and scaling challenges," asserts Malik.

Indeed, investing in high-quality networking equipment from reputable vendors ensures the foundation of a reliable, secure, and high-performance infrastructure. Systems with built-in intelligence enable automated diagnostics, real-time monitoring, and predictive analytics, reducing downtime, simplifying maintenance, and allowing faster resolution of issues resulting in an improved user experience.

"For example, Oxford University deployed a Juniper Mist Wi-Fi network that uses AI to deliver continuous diagnostics and configuration recommendations across all campus access points," highlights Donohue. "This approach ensures consistent performance, strengthens security, and supports growing demands without constant human oversight."

In short, high-quality kit isn't just more reliable — it comes with the intelligence and vendor support needed to keep pace with evolving demands.

Getting smart about traffic

When every device is talking at once, prioritisation becomes non-negotiable.

"Managing bandwidth effectively starts with understanding how traffic moves through a network and applying intelligent controls to keep critical services running smoothly. With connected devices generating constant data, AI-driven analytics can detect congestion, identify performance issues, and automatically allocate resources where they're needed most," explains Donohue.

Quality of Service (QoS) techniques play a key role here by prioritising essential applications such as mission-critical systems or real-time collaboration platforms over non-critical traffic.

"By combining traffic analysis with automated QoS policies, organisations can ensure that their most important services receive guaranteed bandwidth and maintain performance even during peak demand," adds Donohue.

Malik notes that QoS techniques ensure mission-critical apps don't get bogged down: "traffic analysis provides deep insights into how bandwidth is consumed and where congestion points arise, enabling informed decisions about optimisation. QoS then ensures mission-critical applications — such as VoIP, collaboration tools, and business systems — are prioritised over less time-sensitive traffic."

This not only improves user experience but also maximises the value of existing infrastructure by aligning bandwidth allocation with business priorities.

"Advanced network analytics tools and AI-driven telemetry can now automate much of this process, making it easier to dynamically adapt to changing traffic patterns," notes Malik.

Further, uptime doesn't happen by accident; it's engineered.

"Uptime is an architecture choice. Redundancy and failover aren't optional—they're essential for any organisation that depends on uptime," claims Malik. "Protocols like STP, VRRP, and advanced routing convergence mechanisms ensure high availability, preventing single points of failure. This is particularly crucial as more workloads move to hybrid and multi-cloud environments, where network downtime directly impacts customer experience and revenue. Designing redundancy into both the hardware and software layers is the most cost-effective insurance policy for modern enterprises."

"While traditional network protocols like Spanning Tree Protocol (STP) are designed to prevent loops and ensure traffic reroutes in the event of a switch failure, modern smart infrastructure builds on these principles by adding layers of intelligence and automation," adds Donohue.

Security: the invisible backbone of optimisation

If networks are living systems, then monitoring is the pulse check.

Malik explains that "what works today may not meet tomorrow's demands. Continuous monitoring provides real-time visibility into health, utilisation, and security, enabling teams to act proactively rather than reactively. Regular assessments ensure design, performance, and security stay aligned with business growth, regulatory requirements, and evolving threats. Optimisation isn't a one-off project — it's an ongoing discipline."

Donohue echoes this with real-world examples: "in high-footfall public environments like transport hubs, 24/7 remote monitoring of access points and switches ensures consistent availability and quick response to issues. Scheduled maintenance combined with rapid fault resolution helps maintain quality of service. Similarly, in education environments, platforms like Juniper Mist provide AI-driven diagnostics and configuration updates to proactively manage performance. These examples highlight how continuous assessment, supported by intelligent tools, keeps networks reliable, adaptable, and ready for whatever comes next."

Every IT team knows that, as networks become faster and more interconnected, their attack surface grows, making robust security measures more critical

"Next-generation firewalls, intrusion detection and prevention systems (IDS/IPS), and secure segmentation are key pillars of a zero-trust architecture, ensuring that performance improvements never come at the cost of security," warns Malik. "These should be complemented by endpoint detection and response (EDR), anomaly-based analytics, and automated threat response to stop ransomware, phishing, and insider threats in their tracks. In addition, antivirus and anti-malware tools remain essential layers of defence to block and isolate threats before they spread."

Donohue agrees that firewalls and intrusion detection systems are foundational to defending against modern cyber threats, providing the first line of defence, with firewalls controlling access and blocking malicious traffic, and intrusion detection systems monitoring activity across the network to identify and alert on suspicious behaviour.

"In sectors like education, where cybercrime incidents have surged and the industry now ranks among the top five global targets, these protections are more important than ever," shares Donohue. "AI-enhanced security adds a further layer by offering real-time visibility into who is accessing the network, from where, and under what conditions, giving IT teams the insight needed to detect, assess, and respond to threats before they escalate."

Technology alone, however, is not enough: comprehensive user training is vital to build a human firewall, empowering staff to spot phishing emails, social engineering tactics, and other malicious activity.

"A truly optimised network is not only fast and scalable but inherently resilient, with both technical safeguards and well-informed users acting as front-line defenders," comments Malik.

The takeaway? An optimised network isn't just fast — it's resilient against evolving threats.

The bottom line

From scalable design and intelligent traffic management to security-first architectures and continuous monitoring, the principles of network optimisation are clear: plan for growth, invest wisely, automate wherever possible, and never treat optimisation as 'finished.' ■