Operators must do more to ensure IP network resilience

February 2024

Simon Sherrington

IP networks underpin most of the services we take for granted: messaging, voice, online shopping, taxi and train booking, use of social media, watching online TV and video, and online banking. IP infrastructure underpins fixed and mobile networks, enterprise and government networks. Therefore, when IP networks fail, the consequences can be significant. There have been numerous cases of IP network failures that have resulted in loss of services for millions of people and organisations, and that have even prevented calls to emergency services.

Analysys Mason attended Huawei Connect in Shanghai in 2023 to present the findings of its perspective paper *Ensuring IP network resilience*. The paper is based on a detailed survey of IP network operators, and an analysis of causes of IP network failures, and the processes and tools that organisations use to prevent them. The paper shows that there is much more work to be done to improve IP network resilience; and the context of the event itself illustrated that the importance of improving IP network resilience is only going to increase.

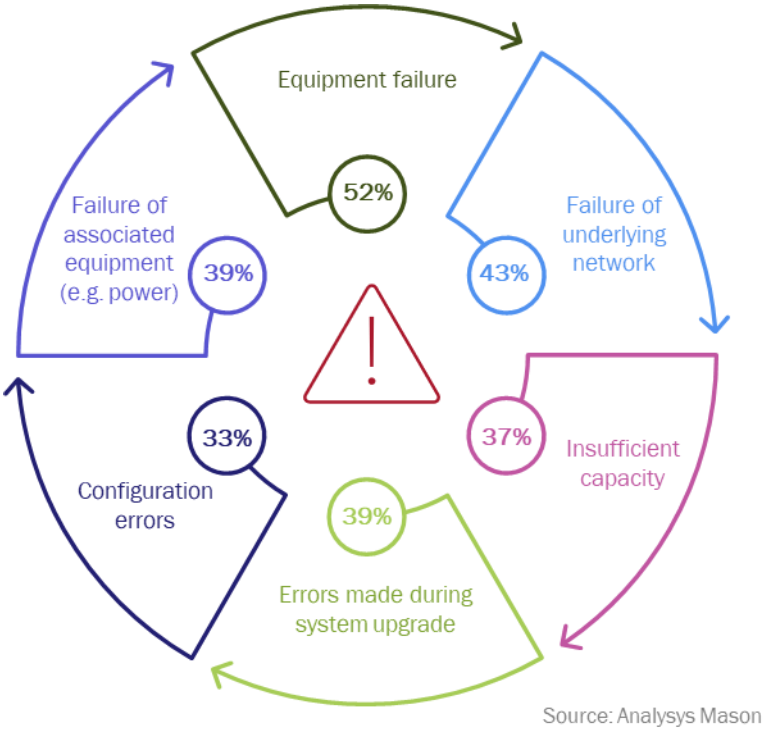
Huawei used its Connect event to set out its vision for AI and how it has the potential to transform industries. Huawei is aiming to build a connected computing backbone, with AI-based analytics available to all, and delivered as a service (inference-as-a-service). It anticipates that its AI computing backbone, comprising network infrastructure, compute and models (ranging from the industry-specific to generic), will supercharge China's productivity and innovation. The plan is the latest announcement in what has become a global AI innovation race. Governments and businesses are all seeking to gain competitive advantage by leveraging AI as it is now, and as it promises to become. However, remotely-hosted AI systems such as the one outlined by Huawei are only as robust as the networks (including IP) that they rely on for the connections between end users and the cloud systems. With the remote hosting of the intelligence needed to manage processes and systems, organisations' future ability to take time-critical decisions will rely on the resilience of IP networks, and the problem is that IP networks are not always designed with resilience in mind.

IP network failures from multiple causes are damaging operators' businesses

Failure to ensure IP resilience is damaging operators' businesses now. Nearly 70% of the respondents in Analysys Mason's survey of IP network operators stated they had lost customers due to IP network outages, and 63% said they have had to pay compensation or damages to their customers following IP network outages. The losses reported by the operators as a result of IP outages ranged from a few million dollars over 12 months to more than USD250 million. The biggest outages are widely reported on, and discussed by, members of the press and media, and sometimes within political circles, so they can cause a lot of brand damage beyond the immediately affected customer base.

Operators cite a wide range of reasons for historical IP failures (Figure 1). Some are caused by equipment failure. Many are caused by human error. These are impossible to manage effectively in isolation and it is important to do much more than simply monitor availability and fix issues as they arise.

Figure 1: Common causes of IP network downtime[1]


Equipment failure
52%
Failure of underlying network
43%
Insufficient capacity
37%
Errors made during system upgrade
39%
Configuration errors
33%
Failure of associated equipment (e.g. power)
39%

Source: Analysys Mason

The results of the survey demonstrate quite clearly that IP network failures are causing economic and reputational damage to operators' businesses, and that exist methods for ensuring resilience are not working. A rethink is needed. Operators need to take a much more strategic approach to IP network resilience. They need to plan resilient network architecture that ensures their IP networks can sustain sufficient network service levels in the face of unexpected or extraordinary occurrences.

Operators need to plan for resilience

Operators need to design-in resilience at the network planning phase. This means architecting the network to avoid problems, or in such a way that problems can be mitigated without affecting customers. Operators must pay attention to a range of factors including (but not limited to) network structure, device configurations, service topologies and requirements, traffic flows and operational processes.

Operators should assess their own resilience, and compare themselves against their peers. This could include evaluating factors such as ability to resist outages, impact on services (with attention paid to the different resilience requirements of different service types), recovery times, ability to prevent problems from cascading or spreading, ability to visualise the network and what is happening, as well as evaluation of operational and management processes and how they can improve resilience. Ideally this review would use an industry-recognised resilience maturity model to ensure it is sufficiently robust.

Digital twin technology can help. An exact digital replica of the real network can be used to test the impact of events such as poorly executed network changes or device reconfigurations, traffic spikes or even malicious attacks. It can also be used to evaluate the ability of the network (and importantly the services it is delivering) to

[1] Question: "Which of the following have caused IP network outages?" 46 respondents, all representatives of operators that operate IP networks.

survive in the face of multiple unexpected events. Use of a digital twin can support a structured process to review the resilience of a network and to redesign/reconfigure it to minimise the likelihood of downtime.

Analysys Mason’s perspective paper, *Ensuring IP network resilience*, offers a detailed view of the challenges faced by operators, and the steps they should take to reinforce the resilience of their IP networks.