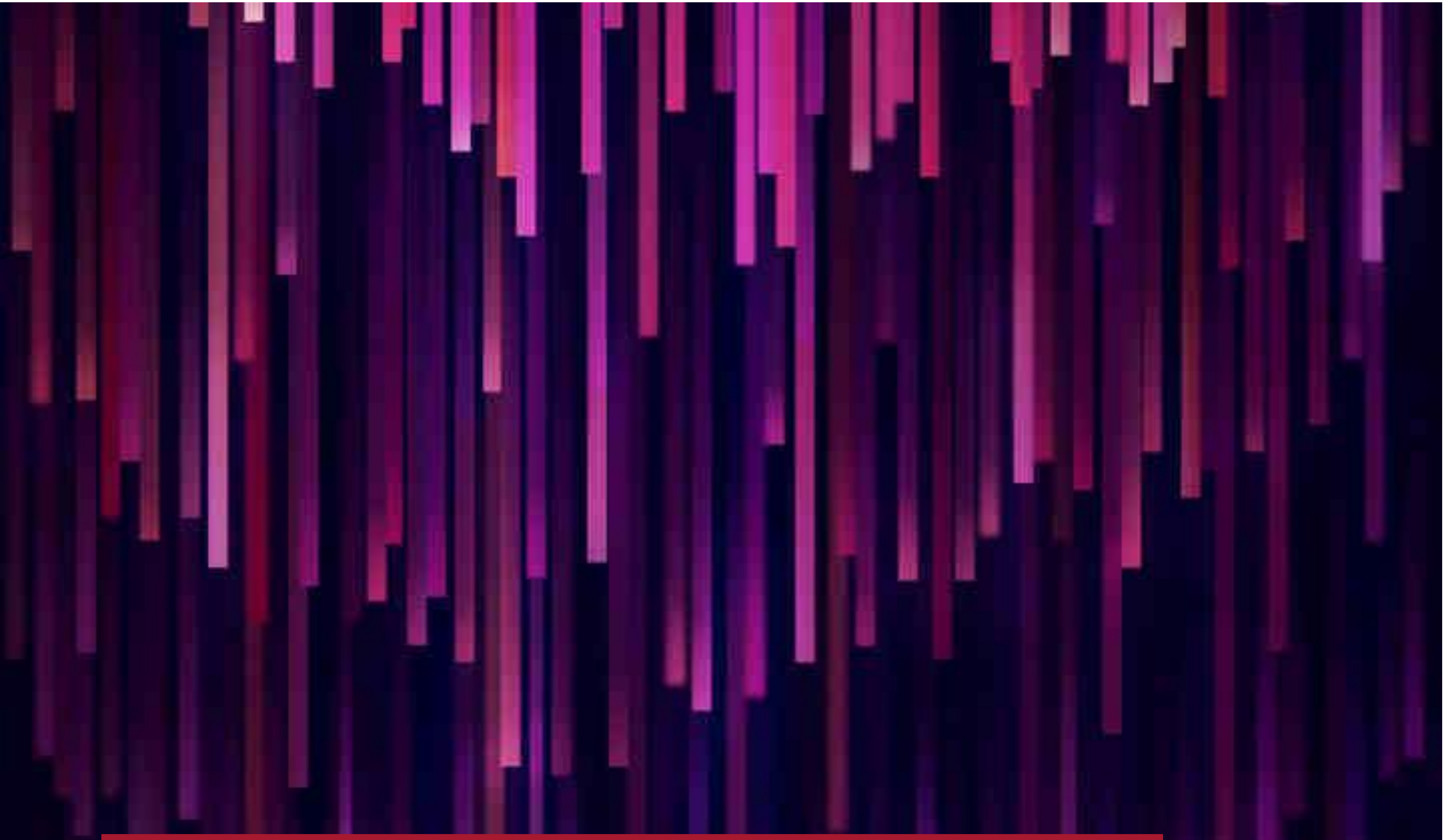


Perspective

Ensuring IP network resilience

September 2023

Simon Sherrington

Contents

List of figures

This perspective was commissioned by Huawei. Usage is subject to the terms and conditions in our copyright notice. Analysys Mason does not endorse any of the vendor's products or services.

This perspective contains the details of information on T/ZGTXXH072—2023, *IP Network resilience specification for computing network convergence network infrastructure*, with contributions from (1) China Academy of Information and Communications Technology; (2) Huawei; (3) Research Institute of China Unicom; (4) Research Institute of China Telecom; (5) Computer Network Information Center, Chinese Academy of Sciences. We received details of the specification from Huawei. We have used reasonable and proper care to cross-check and investigate the material supplied to an appropriate level of detail. Analysys Mason will accept no liability for damages or losses resulting from errors or omissions in materials supplied to us.

1. Executive summary

Most of the digital services used by consumers and businesses run over IP networks, which provide the backbone transport infrastructure for broadband and mobile services and for corporate data networks. The largest national networks operated by telecoms service providers connect thousands of network elements, hundreds of millions of consumer and business customer devices and billions of IoT devices. The IP networks operated by large organisations such as banks underpin the critical digital infrastructure that enables those organisations to function. IP networks interconnect the data centres of the largest internet content and application providers that are used by billions of people daily.

Therefore, when parts of an IP network fail, the implications can be significant. Outages have taken broadband and mobile services offline, cut entire countries off from the internet, prevented financial institutions from processing payments, stopped large social media companies from providing services, and prevented people from making calls to emergency services. Large failures of IP networks can have grave consequences and can also be very costly. Yet IP network outages happen remarkably frequently.

This all clearly demonstrates that organisations need to invest in increasing the resilience of their IP networks. Ensuring network resilience means being certain that service levels can be maintained to an acceptable level in the context of extraordinary events. These events might include equipment failures, malicious attacks or human error. Ensuring resilience is not the same as monitoring reliability. Nor does it mean ensuring network security. Ensuring resilience means taking a strategic approach to improving the robustness of the network by improving its architecture and configuration, in order to pre-empt and prevent problems. It involves building in resilience by design.

Despite the negative implications of IP network failures, many organisations are not doing everything they can to pre-empt and prevent problems. In response to a survey of operators of IP networks conducted by Analysys Mason in August 2023[1], fewer than half of respondents (43%) stated they undertake risk analysis or fault simulation, or network element health checks, only 26% stated they simulate attacks on the network, and fewer than 20% said they undertake fault survivability or disaster recovery analysis.

A range of barriers are preventing operators of IP networks from doing more to ensure IP resilience. These include lack of in-house expertise, lack of budget and time, or inability to observe what is happening within the network. Insufficient expertise is particularly important; human errors cause a great number of outages – for instance, during system upgrades or system reconfigurations.

Traditional approaches to improving IP network resilience are not working. Organisations need to consider a new approach. Given the scale of the risks, and the potential benefits from improving IP network resilience, operators need to adopt a strategic approach. They need to strive for IP network resilience by design – ensuring that resilience is built in at the network planning phase, and that the network architecture, device configurations, service constructs and operational processes are all designed to avoid problems, or to mitigate them without affecting customers.

[1] The survey comprised 23 respondents, all working for companies that operate IP networks, which have experienced some kind of failure of outage. All these companies also generated at least USD500 million annual revenue, with 22% of the companies generating over USD20 billion in revenue.

Organisations can benchmark their level of resilience and measure the progress of their initiatives to improve the resilience of their IP networks by using a resilience maturity model. The model should detail metrics and assessment criteria specifically designed to ensure network resilience and enable an organisation to evaluate the level of IP resilience for different sections of its network.

IP network operators should deploy tools and services that support detailed visual analysis of the IP network. IP resilience by design requires a 360^{O} view of equipment, configurations, network topologies, traffic flows and service utilisation. It requires the ability to analyse the potential impact of equipment, system, configuration, traffic or service changes, failures or malicious attacks. Operators of IP networks should invest in a single tool that enables detailed visualisation of a digital twin of the network.

Organisations can use the digital twin of the network to test complex scenarios and evaluate the performance and resilience of the network in the context of a range of threats, problems and failures. By using a digital twin that matches the real-world network, the testing and evaluation can be undertaken in a safe environment, before the live system is altered. The twin network can be used to test new network architecture and configurations, so that problems can be anticipated and avoided, improving business continuity and business outcomes.

2. IP network operators must pay more attention to network resilience

- Crucial role and increasing complexity of IP networks
- Examples of major outages suffered by operators of IP networks
- Damage and losses caused by outages, including survey data

2.1 IP networks play a crucial role in underpinning critical applications and services

IP networks underpin communications services worldwide, providing the backbone transport infrastructure for broadband and mobile services and for corporate data networks. IP networks serve huge numbers of devices. The largest national networks operated by consumer service providers connect thousands of network elements, and hundreds of millions of consumer and business customer devices, and billions of IoT devices. The IP networks operated by large organisations such as banks underpin the critical digital infrastructures that enable those organisations to function. IP networks interconnect the data centres of the largest internet content and application providers that are used by billions of people daily. IP networks underpin many of the networks that enable emergency services communications so if they fail, people cannot easily call for assistance in times of emergency. IP networks are part of the critical infrastructure of any large communications service provider, government or large enterprise. Without IP networks people cannot access the services on which they rely.

Despite the importance of IP networks in ensuring global digital connectivity, and despite the fact IP networks are used to support increasing numbers of services (such as streaming services and gaming for consumers, or mission critical national and business services) that do not tolerate poor network performance, IP networks are best-effort networks, not originally designed to guarantee service levels. They are reasonably robust – but are based on an infrastructure designed to enable global signalling, addressing and traffic routing, with decisions made locally based on the information received from other parts of the network. This makes them liable to propagate problems if configured incorrectly. IP networks are designed to use statistical multiplexing and best-effort forwarding. Routes are chosen hop-by-hop (by the router) and based on availability of routes. Traffic is prone to congestion, which can cause delay and packet loss. There is little overall control and visibility.

At the same time, IP networks are becoming increasingly complex. The capabilities of devices range from on-premises user equipment capable of serving a single home or branch office, to multi-gigabit or terabit devices residing in operator and enterprise core networks. IP networks rarely contain equipment from a single vendor. They are typically multi-vendor environments. Devices also vary substantially in the protocols they run (for example IPv4 or IPv6). Corporate networks can run to hundreds of thousands of devices; service provider networks can include millions of devices.

Enterprise and government networks are also changing to accommodate new ways of architecting and operating IT systems to deliver services. The IP networks being operated by large organisations such as banks are evolving to include applications hosted in multi-cloud environments encompassing public and private cloud solutions, and the applications are managed or delivered from data centres distributed across multiple locations. These distributed cloud and data-centre architectures require responsive, highly resilient and highly secure networks to ensure that services can be accessed by employees at central and remote or branch sites, as well as by customers 24 hours a day, 7 days a week.

IP networks are also being used in more complex ways. Operators of IP networks are introducing services and applications that require end-to-end visibility and service management. Traffic engineering can be deployed to ensure quality of service for selected customers, services, applications or routes. Multiple overlay systems (for example, IP domain controllers, network management systems and SDN layers) can be used to influence how the network operates or how it manages traffic.

However, there remain significant challenges in seeing and understanding what is happening throughout the network – whether at physical, protocol, slice and service layers. The scale and complexity of IP networks is too great for human minds to be able to understand in sufficient detail. This makes it increasingly difficult to ensure their resilience.

2.2 Failures can lead to substantial outages

IP network failures can cause large-scale and lengthy outages of services that affect millions of users, sometimes for many hours. Public examples of major outages include the following.

- Operator A in Canada (July 2022) – a Canada-wide service outage lasting nearly 20 hours caused by a router misconfiguration. The outage affected tens of millions of customers and led to the loss of cable, fixed telephony and wireless network services – including loss of ability for customers to call emergency services.

- Operator B in Japan (July 2022) – a huge outage affecting more than 30 million mobile phone users as well as critical business services (such as ATM, delivery and weather systems) for more than 3 days. The outage was caused by a router misconfiguration in the core transport network during routine maintenance, which caused a cascade of problems. The misconfiguration disrupted the location registration function within the VoLTE network (devices must register their locations to make VoLTE calls). This triggered numerous retransmissions which in turn caused traffic congestion. Distributed processing caused further spread of the congestion. To make matters worse, the subscriber database became overwhelmed. VoLTE nodes and the mobile packet gateway must authenticate for each call – each retransmission led to a new request and led to data inconsistencies at the subscriber database. This triggered more problems. It took Operator B in Japan more than 72 hours to fix the outage.

- In October 2021, Operator C in in South Korea suffered a network-wide outage preventing the operation of fixed and mobile services for more than an hour. The loss of service affected schools, health services, financial trading organisations and consumers. The outage was initially attributed to cyber attacks, but the operator subsequently confirmed that a border gateway protocol (BGP) configuration error had caused the downtime.

- In April 2020, a Border Gateway Protocol (BGP) configuration error believed to have been caused by a BGP optimiser led to traffic relating to 8000 prefixes (including those relating to Akamai, Amazon, Cloudflare Facebook and Google) being routed through Rostelecom's network in Russia and then black holed. Although Rostelecom revoked the routes, they had already been propagated to peers by some other ISPs. Problems continued for around 5 hours.[2]

- In January 2020, the national provider of Gambia, Gamtel announced a total internet outage affecting the entire country for more than 8 hours. The failure was caused by a faulty network card on the backup link – itself commissioned due to problems with cable cuts to the main submarine cable linking the country to the internet.[3]

The European Union Agency for Cybersecurity (ENISA) reports on network security incidents in the region. Its report *Telecom Security Incidents 2021* states that network operators in Europe reported 168 incidents and the loss of over 5 billion user hours of service in 2021. The main assets affected by security incidents were addressing servers (23%) and switches and routers (18%). Switches and routers have been the largest causes of incidents for 5 years, accounting for 18% of all incidents reported to ENISA between 2017 and 2021.[4]

Outages caused by IP network problems are not limited to telecoms service providers. In October 2021, Facebook (now Meta) suffered outages of its Facebook, Instagram, Whatsapp and Messenger platforms for billions of users for hours. In a public statement, it said the failures were caused by configuration changes to the backbone routers that co-ordinate traffic between its data centres. IP network problems are also known to have caused outages at financial institutions and other major critical national infrastructure providers – although the root causes are not typically made public.

2.3 IP network failures cause significant damage and financial cost

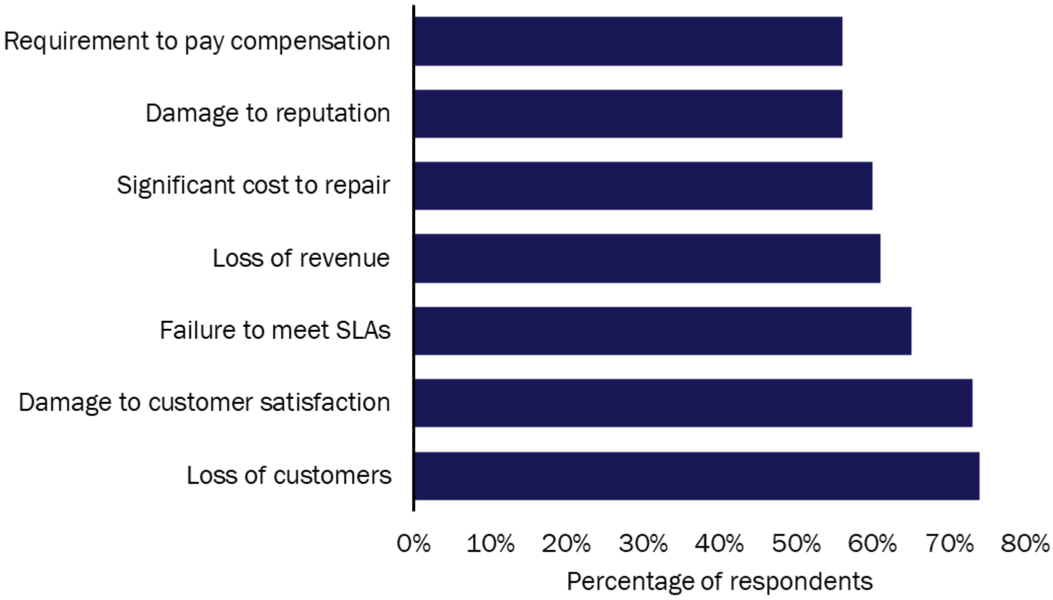
Analysys Mason conducted a survey of operators of large IP networks in August 2023 to understand the extent and impact of IP network failures. The responses show that IP network failures can have significantly damaging implications for organisations. 74% of the organisations surveyed reported IP network failures had caused loss of customers, and 73% indicated IP network outages had damaged customer satisfaction. 57% of the respondents indicated that they had been required to pay compensation to customers as a result of IP network failures.

[2] Rostelecom's Route Hijack Highlights Need for BGP Security (thousandeyes.com)

[3] The Gambia's Internet Outage Through an Internet Resilience Lens (internetsociety.org); https://twitter.com/Gamtel/status/1478310096639770625

[4] https://www.enisa.europa.eu/publications/telecom-security-incidents-2021?v2=1

Figure 2.1: Types of damage caused by IP network outages – percentage of respondents admitting each damage type[5]



Source: Analysys Mason

The scale of losses can be substantial. Following its outage in July 2022, Operator A in Canada experienced significant public backlash, and subsequently committed to a 3-year CAD10 billion programme of investment to improve its network resilience. Operator B in Japan also suffered financial consequences. Nearly 2.8 million customers who were unable to use services for more than 24 hours were eligible for a deduction of 2 days of their subscription charge from their monthly bill, and more than 36 million customers had JPY200 deducted from their bills.

Damage caused by IP network failures are not limited to public examples. When asked about the worst IP network failure at their organisation over the last year[6], the companies surveyed by Analysys Mason, indicated that the worst outages they had experienced over the previous 12 months had affected substantial numbers of customers. Nearly half of respondents said the outage had affected 40% of customers or more. The scale of financial costs of those individual outages often exceeded USD20 million and in one case exceeded USD100 million.

[5] Question: "What impact have IP network failures had on your business? (IP network failures have never caused this / have sometimes caused this / have often caused this)."

[6] Question: "Thinking about the worst IP network outage you have suffered over the last year, please estimate:

- How many hours were services down? Enter the number of hours.
- What was the percentage of customer affected? Enter the percentage value.
- What was the total cost (including lost revenue, compensation to customers, and cost to fix)? Enter the cost in units of USD million."

Figure 2.2: Percentage of customers affected by each surveyed company's worst network outage over the last year[7]

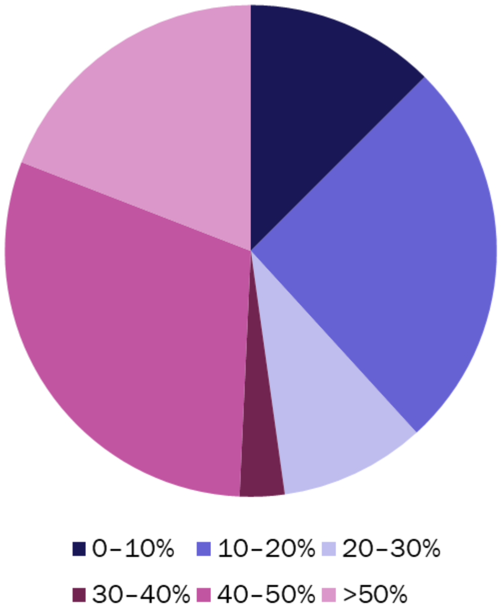
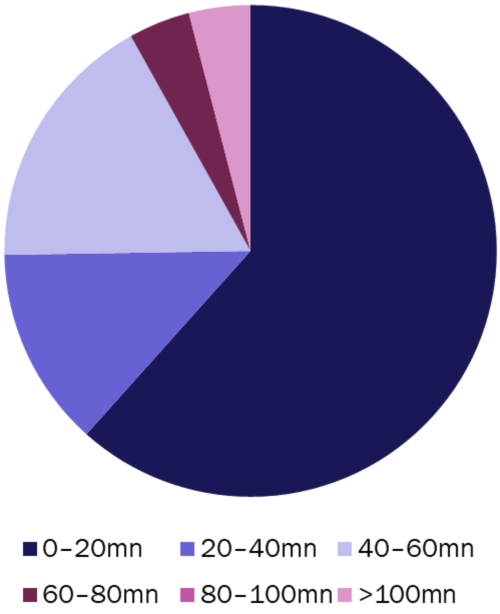


Figure 2.3: Total cost (USD) of each surveyed company's worst network outage over the last year[8]



Source: Analysys Mason

The survey results demonstrate that ensuring IP network resilience must be a critical component of an IP network operator's strategy or significant damage can be caused.

3. Traditional approaches to prepare for and pre-empt network incidents are not optimal

- Gaps in systems and processes used by organisations with IP networks, including survey data
- Organisational barriers to improving IP network resilience, including survey data

3.1 There are many gaps in organisations' IP resilience assurance strategies

Analysys Mason's survey of IP network operators shows that companies employ a wide range of approaches to ensuring IP network resilience. IP network audits are typically conducted at least once per month (69%), with ~26% claiming they conduct such checks on an ongoing basis. This highlights the fact that most companies are

[7] Does not sum to 100% due to rounding.

[8] Does not sum to 100% due to rounding.

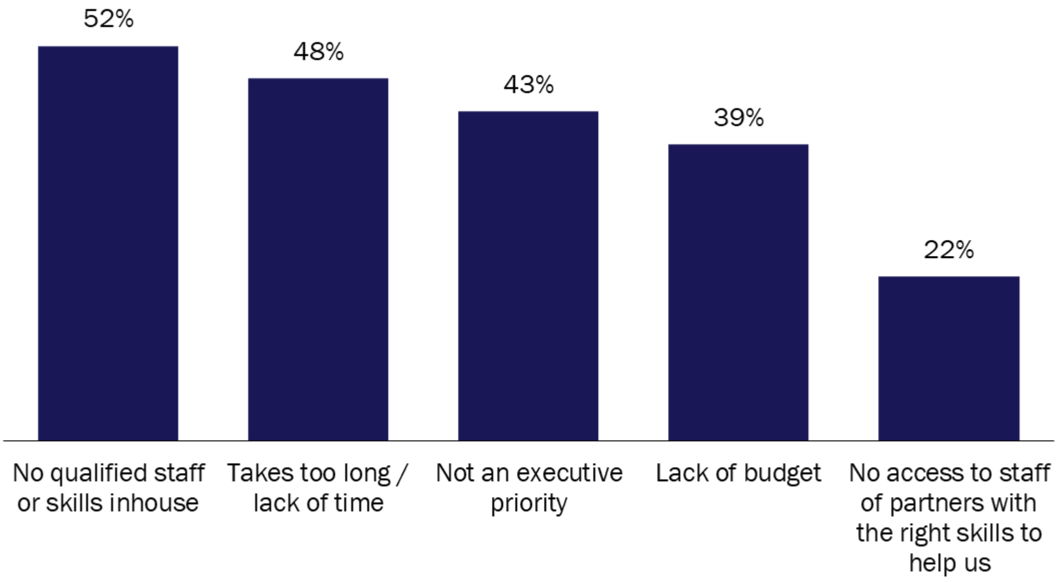
at least somewhat proactive in the practice of audit. However, the survey results also reveal significant gaps in auditing processes.

Significantly, only around half of all respondents to Analysys Mason's survey reported[9] that they systematically undertake network topology analysis or IP optimisation analysis, fewer than half (43%) undertake risk analysis or fault simulation, or network element health checks, only 26% simulate attacks on the network, and fewer than 20% undertake fault survivability or disaster recovery analysis.

3.2 Organisations face substantial barriers to ensuring IP network resilience

Companies are hindered in their ability to ensure resilience of their IP networks by a range of organisational and technological factors. Organisational barriers to improving IP network resilience include the lack of in-house skills (cited by more than 50% of all respondents), as well as time and lack of budget. 43% of respondents also stated that preventing IP network outages was not a priority for executives within their company.

Figure 3.1: Organisational barriers to ensuring IP network resilience[10]



Source: Analysys Mason

Technological barriers also prevent companies from improving their IP network resilience. The barriers most commonly cited by the respondents to Analysys Mason's survey included inability to observe IP network behaviour in sufficient detail (74% of respondents) and lack of real-time information (52% of respondents), with a range of other factors (such as lack of insight into topology, service performance and individual device configurations) cited by 43% of respondents.

[9] Question: "Which of the following activities do you undertake to pre-empt and prevent failures? Select all that apply."

[10] Question: "What factors have hindered or limited your ability to prevent IP network outages? Select all that apply from the list of organisational factors."

3.3 A new approach is needed

It is clear that organisations understand the importance of their IP networks for underpinning their services and their customers' services, and it is clear they are taking a range of measures to sustain services when unexpected events occur. However, traditional approaches to ensuring network resilience are leaving gaps and weak points, and are failing to prevent serious network outages. A new strategy is clearly needed. Organisations need to consider a broader programme of measures including evaluation and measurement across a wide range of performance indicators, adoption of new resilience evaluation methods, and the introduction of tools enabling improved and much more granular visualisation of what is happening (or could happen) in the network. They should also consider benchmarking the resilience of their network against a structured framework, so they can clearly judge the resilience of their systems.

4. Organisations need to ensure network resilience from the network planning stage

- The need for resilience by design
- The benefits of creating a digital twin
- Using a resilience maturity model to evaluate IP network resilience
- Using the digital twin to evaluate the architecture for weak points and test extraordinary events

4.1 Ensuring network resilience means ensuring that services can continue in extraordinary circumstances

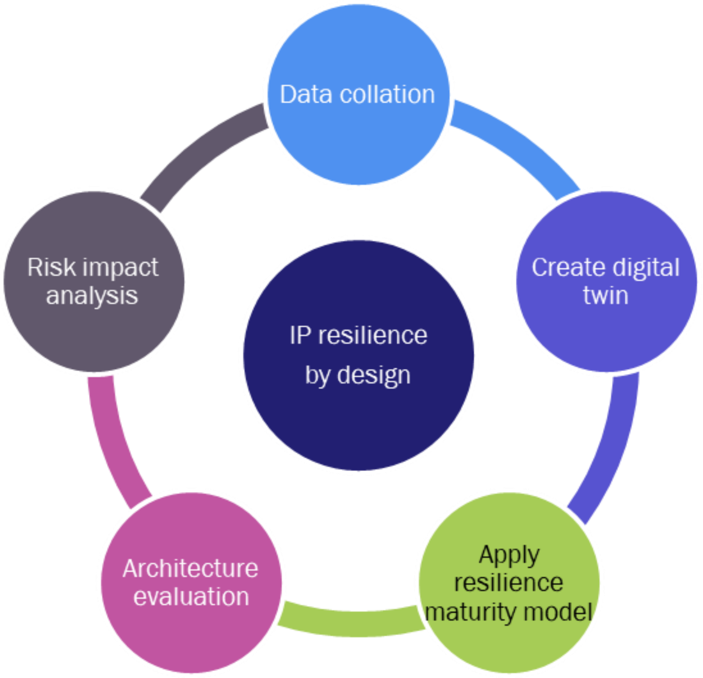
The evidence clearly demonstrates that organisations need to invest in increasing the resilience of their IP networks if they are to avoid the catastrophic failures and damage to their businesses that can result from network outages.

Ensuring network resilience means being certain that service levels can be maintained to an acceptable level in the context of extraordinary events. These events might include equipment failures, malicious attacks or human error. Ensuring resilience is not the same as monitoring reliability. The network can have a very high level of reliability most of the time but may still fail very badly when things go wrong – especially when problems cascade throughout the infrastructure. Nor does it mean ensuring network security – which is also critical. Ensuring resilience means taking a strategic approach to improving the robustness of the network by improving its architecture, and configuration to pre-empt and prevent problems. It involves building in resilience by design so that when security issues occur, or when events happen that cause issues within the network, those issues can be mitigated, contained and resolved in the fastest possible time, with the minimum disruption for services and customers.

4.2 Operators of IP networks need to 'design-in' resilience

It is critical for operators of IP networks to put in place robust strategies that enable them to identify the root causes of problems, to fix issues quickly, to implement architectural or configuration changes that reduce the likelihood of future outages, and to make the IP network more resilient when issues arise. Simply monitoring uptime and service availability levels is not sufficient. Relying on people not to make errors under pressure is not sufficient. Operators of IP networks need a comprehensive programme of data collection, visualisation, analytics and IP network refinement – all benchmarked against clear metrics, and they need to pre-empt causes and model solutions.

Figure 4.1: IP network resilience by design



Source: Analysys Mason

The starting point for this process is for operators to understand their current network architecture and configurations, and to be able to visualise them.

4.3 Combining data spread across multiple silos can support detailed analysis

An initial step for IP network operators to take is to gain a detailed understanding of the current state of their IP infrastructure. This requires data collection for individual network elements, IP network topology and behaviour, and services running over the network.

Individual network elements need to be audited for factors such as configuration, location and utilisation levels. The audit must encompass devices at end-user premises as well as those within the core IP network. Given the mix of ages, types and locations of network elements within a large IP network, it is likely that some of the data collection and aggregation will need to be undertaken manually, using a variety of systems.

Configuration is a particular challenge given that thousands of devices might need to be audited. Ideally, the configuration of the devices would be checked against a database of known configuration issues and the process would be undertaken automatically using a software-based approach. The manual alternative would be very time-intensive. This is an important part of any resilience improvement strategy as configuration errors are known to have caused significant errors in IP networks.

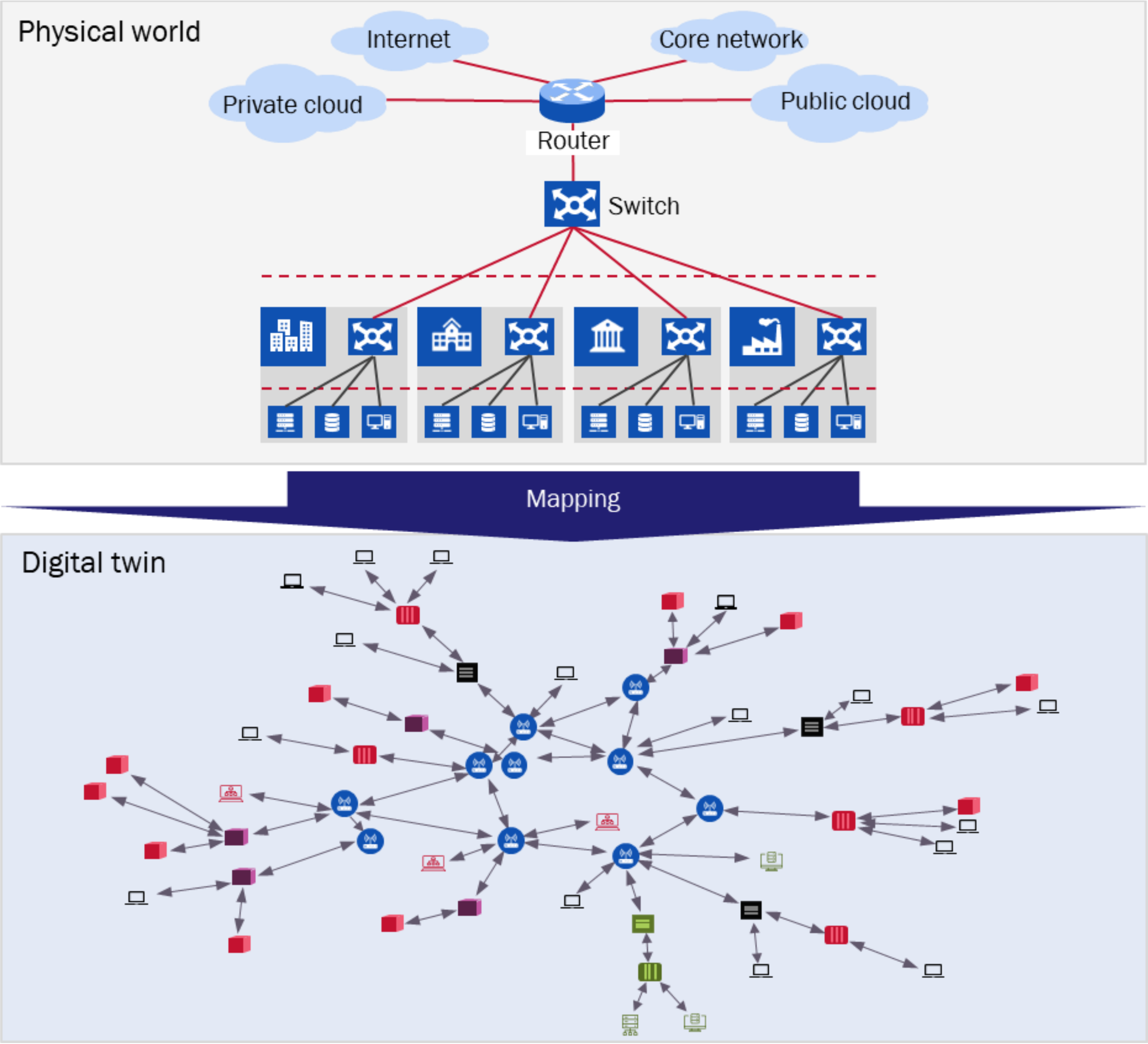
The data can then be brought together within a visualisation tool to enable analysis.

4.4 Creating a digital twin of the network enables advanced visualisation and evaluation

In most cases, the data needed to undertake a detailed assessment of the resilience of an IP network is likely to reside in various data silos and across multiple systems. Analysys Mason's survey shows that few IP operators have a single tool they can use to undertake sophisticated, holistic element, topology, traffic and service analysis. 74% of the companies surveyed stated that inability to observe network behaviour in sufficient detail is a barrier to ensuring and improving IP network resilience.

One approach to overcoming this is to use software and advanced visualisation techniques to build a digital twin of the IP network (Figure 4.2).

Figure 4.2: Digital twin of an IP network



Source: Analysys Mason

Creation of a digital twin means integrating all relevant data sets within a single tool and using advanced visualisation techniques to create a holistic digital version of the network. This maps the physical world onto the digital world.

The digital twin enables visualisation of all the network elements, physical and logical topologies, traffic utilisation levels and flows. With a detailed understanding of what is happening within the IP network, it is possible to identify weak points, and to identify opportunities to increase the resilience of the network. The digital twin can also be used to analyse network resilience under a wide range of possible scenarios by simulating malicious attacks, service provider failures, environmental disasters, equipment failures and operational or configuration errors. The simulations will identify additional weak points, or opportunities for optimisation, and the learning from those simulations can be used to make further improvements to the real-world network.

Critically, creation of a digital twin enables evaluation of potential threats and their impact on services, before the changes are made within the network itself. Human failures are a significant cause of IP network outages. ENISA's report identified human error as the cause of 23% of all incidents it reported and those incidents were typically catastrophic, accounting for 91% of all hours lost. Analysys Mason's survey of IP network operators also investigated causes of IP network failures and outages. This also confirmed the impact of human activity. While equipment failures feature highly in causes of failure cited by survey respondents, so too does human mistakes; 57% of respondents reported outages caused by errors made during system upgrades and 39% reported outages caused by errors made during reconfigurations. Using a digital twin could enable IP network operators to avoid some of the human-induced errors. An organisation can test network adjustments, optimisation and maintenance activities in a safe environment – before adjustments are made to the live network.

4.5 Evaluation of IP resilience against a resilience maturity model can show where improvement is needed

Organisations can measure the progress of their initiatives to improve the resilience of their IP networks by tracking their performance against an IP resilience maturity model. One example of an IP resilience maturity model has been developed by the China Institute of Communications (CIC).[11] It has drafted a specification that is applicable to all types of IP network operator. It is designed to assure resilience during five operational phases: prevention, detection, response, recovery and ongoing adaptation.

The specification envisages five levels of resilience (level 5 is the most resilient) and recommends different parts of the network should be targeted to achieve different levels of resilience – for instance, core networks should achieve resilience level 5 whereas standard internet services should achieve resilience level 3 or above.

The specification recommends evaluation of resilience in six areas (Figure 4.3).

Figure 4.3: Model for evaluating IP resilience

	Level 1	Level 2	Level 3	Level 4	Level 5
Impact resistance	0	1	2	3	4
Service impact	>30%	<=30%	<=20%	<=10%	<=5%
Recovery speed	Days	Hours	Minutes	Seconds	Microseconds
Fault limitation	Whole network	Whole network	BGP domain only	IGP domain only	Single site
Management structure	Weak	Relatively weak	Relatively strong	Relatively strong	Strong

[11] More details are available from https://www.ttbz.org.cn/StandardManage/Detail/84652.

	Level 1	Level 2	Level 3	Level 4	Level 5
Visualisation capability	Weak	Relatively weak	Relatively strong	Relatively strong	Strong

Source: The China Institute of Communications

The specification sets out detailed metrics for analysis in each of those six areas.

- **Impact resistance:** measuring the number of times the network can withstand the concurrent simulated attacks. At level 5 it would be able to withstand four concurrent attacks.
- **Service impact:** measuring levels of service impacted, ranging from >30% of customer services affected to fewer than 5% of customers. More-detailed metrics for evaluation cover service quality (packet loss, delay and hop count), and proportions of customers that have been affected.
- **Recovery speed:** time needed to restore services.
- **Fault limitation:** a measurement of how widely faults propagate. To achieve level 5 status, faults are restricted to a single site. Scoring in this area can encompass measurement of how technologies are deployed and the software protocols that have been activated, covering factors such as software and hardware patch deployment; deployment of anti-loop protocols at layers 2 and 3; layer 2 and layer 3 fault domain isolation, and BGP fault isolation.
- **Evaluation of management structure** in areas such as physical separation of business operations, network management and maintenance in the core network; and physical or logical separation of business operations and network management and maintenance in the access network, as well as account log-in policies.
- **Visualisation capability:** ability of the IP network operator to visualise network topology and network service path in real-time; to monitor routers and interior gateway protocol (IGP) and BGP activity and alarms in real time; and view real-time network quality across metrics such as latency, bandwidth and packet loss.

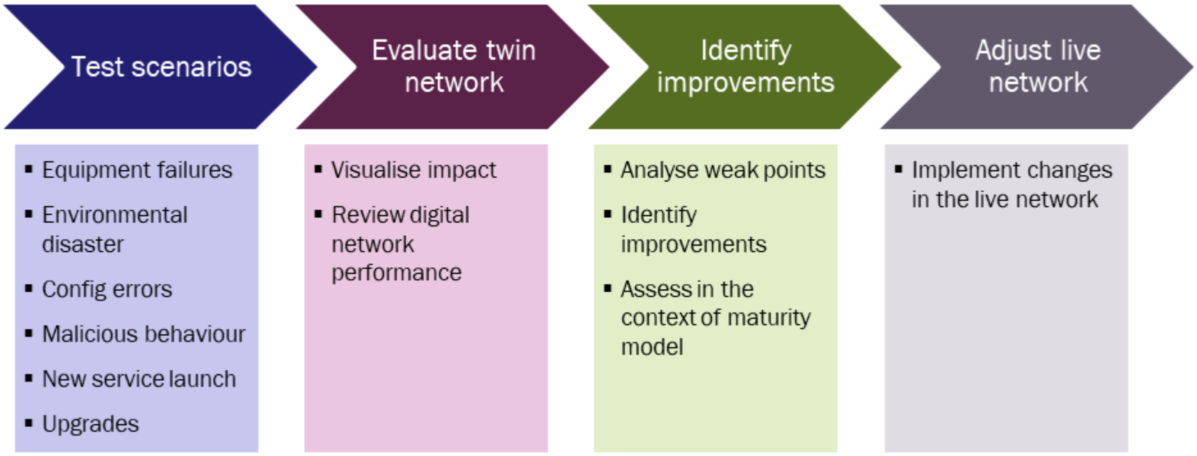
The specification sets out detailed scoring mechanisms for each of these areas.

With a model that can be used as an evaluation framework, an organisation can assess its starting point, and can monitor its progress in improving the resilience of the IP network.

4.6 Dynamic testing with real-network data can support IP network refinement

By using a digital twin of the live network, an operator can test the behaviour and resilience of the network under a range of scenarios (Figure 4.4). It becomes possible to visually analyse the risk and impact of extraordinary events that might cause parts or all of the network to fail, or to operate sub-optimally.

Figure 4.4: IP networks resilience scenario analysis



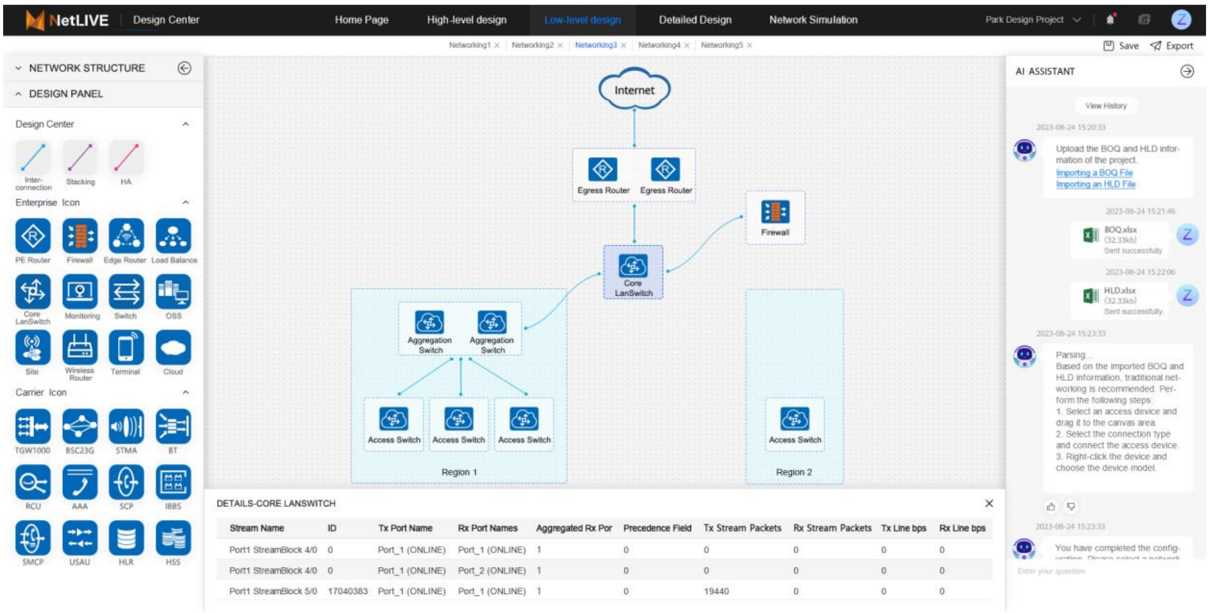
Source: Analysys Mason

A variety of scenarios can be tested by introducing a mix of controlled and uncontrolled disturbances into the digital twin network. These can include the launch of new services, or management of system upgrades, to equipment failures, configuration errors or external causes of failures such as malicious activity or environmental disasters. Ideally, the network can be stress-tested under a range of different scenarios, and the results seen visually by the network planners. The performance of different parts of the network can be evaluated to ensure higher levels of resilience in core areas, and sufficient resilience for less important sites or services.

4.7 The digital twin can be used to test architecture change

Many problems arise because IP network architecture has not been designed to maximise resilience. Single points of failure have caused cascading problems that have led to failure of large sections of an IP network, and the services it supports. Once the digital twin of the network has been developed it becomes possible to review the overall structure of the IP network, with a real-time analysis of topology and the routes used. With advanced visualisation, an IP network operator can undertake a detailed architecture evaluation. It is possible to analyse whether existing structures need to be altered, and whether introducing new hierarchical levels or mesh topologies within the network, or use of IGP/BGP protection mechanisms could improve resilience.

Figure 4.5: Using the digital twin to analyse network weak points



DETAILS-CORE LANSWITCH

Stream Name	ID	Tx Port Name	Rx Port Names	Aggregated Rx Por	Precedence Field	Tx Stream Packets	Rx Stream Packets	Tx Line bps	Rx Line bps
Port1 StreamBlock 4/0	0	Port_1 (ONLINE)	Port_1 (ONLINE)	1	0	0	0	0	0
Port1 StreamBlock 4/0	0	Port_1 (ONLINE)	Port_2 (ONLINE)	1	0	0	0	0	0
Port1 StreamBlock 5/0	17040383	Port_1 (ONLINE)	Port_1 (ONLINE)	1	0	19440	0	0	0

2023-08-24 15:20:33

Upload the BOQ and HLD information of the project.
Importing a BOQ File
Importing an HLD File

2023-08-24 15:21:46

BOQ.xlsx
(32.33kb)
Sent successfully.

2023-08-24 15:22:06

HLD.xlsx
(32.33kb)
Sent successfully.

2023-08-24 15:23:33

Parsing...
Based on the imported BOQ and HLD information, traditional networking is recommended. Perform the following steps:
1. Select an access device and drag it to the canvas area.
2. Select the connection type and connect the access device.
3. Right-click the device and choose the device model.

2023-08-24 15:23:33

You have completed the configuration. Please select a network

Source: Huawei

An IP network operator could review the impact of any architecture changes against its ability to pre-empt and avoid problems, as well as its model for resilience improvement, looking at factors such as service impact, fault limitation and recovery speed. The review could additionally encompass an evaluation of the services running over the IP network including capacity utilisation, review of service-level agreements (SLAs) and quality of experience.

As weak points are identified, the digital twin can be adapted to determine how changes can pre-empt, prevent or minimise the impact of outages, or ensure swifter recovery. Once the changes have been safely tested in the digital twin, the live network can be adapted.

5. Conclusions and recommendations

The evidence shows that IP network failures and outages can have a significant impact on operators of IP networks and their customers. Organisations that do not invest in the resilience of their IP infrastructure can suffer damage to reputation, reduction of customer satisfaction, loss of revenue or customers and the requirement to pay compensation to customers. Large-scale outages happen too frequently, and with significant consequences. Traditional approaches to ensuring network resilience are clearly not working.

Organisations should consider new methodologies and systems for assuring the resilience of their IP networks. The positive benefits of increasing the resilience of the IP network are likely to include improved customer experience, increased customer satisfaction, and avoided costs and damages. As revenue losses will be avoided, investment in improved IP resilience is also likely to lead to increased revenue. In addition, new tools and approaches can help organisations to improve business continuity and avoid issues as they make important investments such as upgrades from IPv4 to IPv6, new service roll-outs or new network deployments.

5.1 Key recommendations

Organisations should take several steps to ensure IP network resilience.

- **Recommendation 1. Take a strategic approach to improving IP network resilience and ensure IP resilience by design.** It is evident that many operators of IP networks are suffering negative impacts from IP networks failures. It is also evident that there are many additional precautionary measures they can take in order to pre-empt and avoid or limit IP network outages. This requires IP resilience by design – ensuring that resilience is built in, and that the network architecture, device configurations, service constructs and operational processes are all designed to avoid problems, or to mitigate them without impact on customers.
- **Recommendation 2. Assess resilience against a maturity model.** Use of a detailed model that sets out targets for resilience, with clear metrics, steps to take, and means of measuring them can help an organisation improve the resilience of its IP network. The model can be used to assess the starting point, and the progress made towards best-in-class resilience.
- **Recommendation 3. Deploy tools and services that provide a holistic view and visual analysis of the IP network.** IP resilience by design requires a holistic view of equipment, configurations, network topologies, traffic flows and service utilisation. It requires ability to analyse the potential impact of equipment, system, configuration, traffic or service changes, failures or malicious attacks. Operators of IP networks have access to many data sets on performance of their IP networks, although these are typically spread across a range of different applications. Operators of IP networks should invest in a single tool or service that enables them to combine data from all the different data sources available to them in a single application. The application should enable detailed visualisation of a digital twin of the network.
- **Recommendation 4. Organisations should undertake detailed scenario testing using the digital twin.** This can enable them to evaluate the network performance under a range of stress conditions, and to experiment with configuration or architecture changes before making them in the live network. They can evaluate the performance of the network – in the context of the resilience maturity model – to determine whether adjustments are required.

6. Annex: Huawei resilient network solution

With the digital and intelligent transformation of enterprises, communication infrastructure is becoming more and more important as the backbone of daily operations. However, the continuous development of services and evolution of network architecture inevitably adds to the complexity of the network. As a result, the risks to network resilience increase, and the network's ability to cope with unexpected impacts decreases.

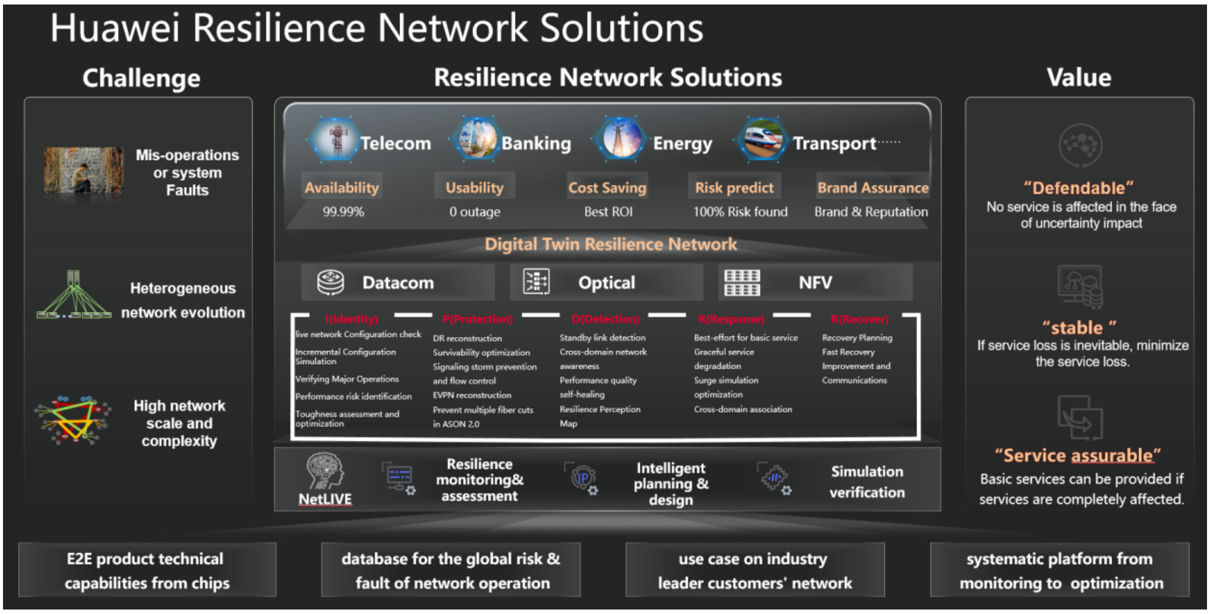
As a leading network equipment and service provider, Huawei is seeking to address industry challenges and explore industry best practices together with partners. Huawei provides solutions that can help IP network providers to ensure their networks are reliable, available and cost-effective.

Huawei's resilient network solution is based on four capabilities:

- the end-to-end capabilities of the technology (from chips and boards to networks)
- the database of risks and faults of network operations
- the network deployments leading industry leaders
- the NetLIVE platform that enables monitoring and network optimisation.

Based on the NetLIVE platform and the Identify, Protect, Detect, Respond and Recover (IPDRR) framework, Huawei has built a set of solutions from identification to recovery, with a view to solving the resilience problems faced by multiple industries, including telecoms, banking, energy and so on (Figure 6.1).

Figure 6.1: Huawei resilient network solution



Huawei Resilience Network Solutions

Challenge

Mis-operations or system Faults

Heterogeneous network evolution

High network scale and complexity

Resilience Network Solutions

Telecom | Banking | Energy | Transport……

Availability 99.99% | Usability 0 outage | Cost Saving Best ROI | Risk predict 100% Risk found | Brand Assurance Brand & Reputation

Digital Twin Resilience Network

Datacom | Optical | NFV

I(Identity): live network Configuration check; Incremental Configuration Simulation; Verifying Major Operations; Performance risk identification; Toughness assessment and optimization

P(Protection): DR reconstruction; Survivability optimization; Signaling storm prevention and flow control; EVPN reconstruction; Prevent multiple fiber cuts in ASON 2.0

D(Detection): Standby link detection; Cross-domain network awareness; Performance quality self-healing; Resilience Perception Map

R(Response): Best-effort for basic service; Graceful service degradation; Surge simulation optimization; Cross-domain association

R(Recover): Recovery Planning; Fast Recovery; Improvement and Communications

NetLIVE | Resilience monitoring& assessment | Intelligent planning & design | Simulation verification

Value

"Defendable" No service is affected in the face of uncertainty impact

"stable " If service loss is inevitable, minimize the service loss.

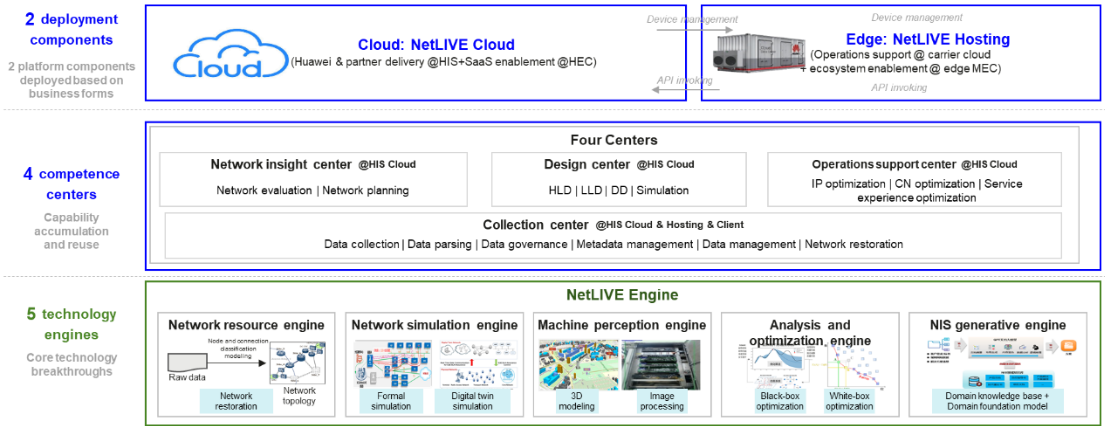
"Service assurable" Basic services can be provided if services are completely affected.

E2E product technical capabilities from chips | database for the global risk & fault of network operation | use case on industry leader customers' network | systematic platform from monitoring to optimization

Source: Huawei

The NetLIVE platform architecture consists of five technical engines and four competence centres. It can be consumed from the centre cloud and the edge cloud (Figure 6.2).

Figure 6.2: NetLIVE platform architecture


2 deployment components
2 platform components deployed based on business forms
Cloud: NetLIVE Cloud
(Huawei & partner delivery @HIS+SaaS enablement @HEC)
Device management
API invoking
Edge: NetLIVE Hosting
(Operations support @ carrier cloud + ecosystem enablement @ edge MEC)
Device management
API invoking
4 competence centers
Capability accumulation and reuse
Four Centers
Network insight center @HIS Cloud
Network evaluation | Network planning
Design center @HIS Cloud
HLD | LLD | DD | Simulation
Operations support center @HIS Cloud
IP optimization | CN optimization | Service experience optimization
Collection center @HIS Cloud & Hosting & Client
Data collection | Data parsing | Data governance | Metadata management | Data management | Network restoration
5 technology engines
Core technology breakthroughs
NetLIVE Engine
Network resource engine
Node and connection classification modeling
Raw data
Network restoration
Network topology
Network simulation engine
Formal simulation
Digital twin simulation
Machine perception engine
3D modeling
Image processing
Analysis and optimization engine
Black-box optimization
White-box optimization
NIS generative engine
Domain knowledge base + Domain foundation model

Source: Huawei

Four competence centres

- Collection centre. Collects, stores and models data for the solution. Makes the data visible to the users.
- Network insight centre. Supports the network insight process and provides capabilities such as network management, network insight requirement management, lead management and milestone management. It builds the cross-domain network evaluation capability, integrates the single-domain network evaluation capability, accumulates network evaluation experience and lowers the network evaluation threshold. Network evaluation reports are managed in a structured and online manner, and are automatically generated.
- Design centre. Supports the completion of network design and mobile network verification activities, outputs scenario-based design documents and verification reports through AI-generate content (AIGC) and intelligent interaction, and supports onsite (remote) delivery and enterprise delivery for capability invoking.
- Auxiliary operation centre. Implements and monitors the Reference Architecture, provides service performance optimisation services based on cloud big data and AI analysis capabilities, and helps customers to increase revenue.

Five technology engines

- Network resource engine. Restores collected network data and stores the data in a structured manner. It describes the status of an operator's network and continuously records the changes. This engine serves as the basis for other engines, providing network specific data foundation for analysis and optimisation. Typical scenarios include network restoration, network modeling and network dynamic database.
- Network simulation engine. Provides formal configuration verification, mechanism-driven modeling, data-driven modeling, hybrid modeling and automatic testing capabilities based on the existing simulation capabilities of the single-domain product line. It is used for deduction analysis in network planning, design, test and change scenarios. Typical scenarios include traffic load impact simulation, service routing and traffic simulation.
- Machine perception engine. Provides capabilities such as image recognition, video acceptance, defect detection, 3D modelling and rendering, and AR rendering. It is used in scenarios such as engineering surveys, visualising designs, and quality inspection and acceptance, and can be extended to various xToB scenarios. Typical scenarios include optical cable dumb resource device detection, digital device modelling and measurement, and industry application defect detection.

- Analysis and optimisation engine. Provides white-box optimisation (one can use mathematical formulas to express objectives and constraints and find the optimal solution), black-box optimisation (one can find the optimal solution by continuously interacting with the simulation system) and big data mining capabilities, which are used to solve the optimal solution in scenarios such as data collection, network planning, design and auxiliary operation. Typical scenarios include site selection solution for the combination of two networks, identification of potential home broadband customers and scheduling of digital logistics workshops.
- Generative engine of network integration service. Accumulates professional network knowledge and Huawei's knowledge of network integration, provides assistance through interactive interfaces, and improves frontline network planning, design and operation efficiency, user data collection, network planning and design, and onsite operations. Typical scenarios include Multi-Vendor IP configuration translation, MOP (method of procedure) document generation and intelligent auxiliary design for enterprise campus networks.

Huawei's NetLIVE-based resilient network solution has provided services for some significant customers and is performing well in multiple fields, such as live network configuration check, disaster recovery reconstruction, survivability optimisation, signalling storm prevention and flow control.

7. About the author

Simon Sherrington (Research Director) leads Analysys Mason's new *Transport Network Strategies* research programme, and its established *Telecoms Strategy and Forecast* programme. He also has a remit to expand Analysys Mason's research forecasts and cross-programme thought leadership. He has nearly 30 years of experience in the industry, having worked as an analyst, consultant, market researcher and publisher. He has commented and advised on many different aspects of the telecoms business during that time. His CV includes a wide range of assignments covering fixed and mobile devices and networks, operator strategies, infrastructure evolution, as well projects encompassing retail and wholesale, and business and consumer services. Simon joined Analysys Mason from Innovation Observatory, a business he founded in 2005 to help clients working in the telecoms, media, IT and environmental technology sectors. Prior to that, Simon worked for Analysys Mason in a number of roles including Head of Custom Research, and early in his career he worked for CIT Publications (at the time a publisher of telecoms and media reports). Simon holds an LLB from the University of Exeter.

Analysys Mason Limited. Registered in England and Wales with company number 05177472. Registered office: North West Wing Bush House, Aldwych, London, England, WC2B 4PJ.

We have used reasonable care and skill to prepare this publication and are not responsible for any errors or omissions, or for the results obtained from the use of this publication. The opinions expressed are those of the authors only. All information is provided "as is", with no guarantee of completeness or accuracy, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will we be liable to you or any third party for any decision made or action taken in reliance on the information, including but not limited to investment decisions, or for any loss (including consequential, special or similar losses), even if advised of the possibility of such losses.