ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(07/2026)

YSTR.nr

Future network resilience use cases and capability considerations

Technical Report ITU-T YSTR.nr

Future network resilience use cases and capability considerations

Summary

Technical Report ITU-T YSTR.nr describes the concept of future network resilience, use cases and root cause analysis, as well as the generic and specific technical considerations of future network resilience.

Keywords

Future network, network resilience, use case.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Technical Report	1
4	Abbreviations and acronyms	1
5	Introduction	3
5.1	Background	3
5.2	General concept of future network resilience	3
6	Generic consideration of future network resilience	5
6.1	Network fault prevention capability	5
6.2	Network awareness capability	5
6.3	Network fault tolerance capability	5
6.4	Network fault containment capability	5
6.5	Network recovery capability	6
6.6	Network resilience re-architect capability	6
7	Use cases and root cause analysis	6
7.1	Use Case 1: Inaccurate network planning and design deficiency	6
7.2	Use Case 2: Impairment of routing integrity and stability	7
7.3	Use Case 3: Router resource exhaustion and control-plane overload	7
7.4	Use Case 4: Network flapping events	8
7.5	Use Case 5: Always-on network management	9
7.6	Use Case 6: Mitigation of signalling storms and snowball effects	10
7.7	Use Case 7: Regional service self-containment	12
7.8	Use Case 8: Over-centralized network element deployment	12
7.9	Use Case 9: Network resilience evaluation and re-architecting	13
8	Specific consideration of future network resilience	13
8.1	Logical routing architecture redundancy and diversity capability	13
8.2	Physical network architecture redundancy capability	14
8.3	Service, routes, traffic and device anti-overload capability	14
8.4	Network topology awareness capability	14
8.5	Network performance awareness capability	14
8.6	Cross-domain network resilience capability	15
8.7	Survival capability	15
8.8	Blast radius optimization capability	15
8.9	Service and network separation capability	15
8.10	Key network nodes and service distribution	15

Page

8.11 Hierarchical and modular design, clean network architecture 16
8.12 Logical layered protocols architecture 16
9 Best practice of future network resilience architecture 16
9.1 Distributed service architecture 17
9.2 Independent Internet core with regionalized Internet contents 18
9.3 Vendor diverse dual-plane national core 18
9.4 Isolated network design principle to optimize Blast Radius 18
9.5 Geo-redundancy and diversity for key services and nodes 18
Bibliography 19

Technical Report ITU-T YSTR.nr

Future network resilience use cases and capability considerations

1 Scope

This Technical Report describes the concept of future network resilience, use cases and root cause analysis, as well as the generic and specific technical considerations of future network resilience.

The scope of this Technical Report includes:

– Concept of future network resilience;

– Use cases and root cause analysis;

– Generic technical considerations for future network resilience;

– Specific technical considerations for future network resilience;

– Best practices of future network resilience architecture.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 IP core network [b-ITU-TY.1231]: IP service provider's network, including one or more IP service providers.

3.1.2 path protection [b-ITU-T Y.1714]: Path protection provides end-to-end protection from source to tail for a given LSP [label switched path].

3.1.3 protocol layer [b-ITU-T Q.1290]: A group of one or more functions within an upper and lower logical boundary within a protocol reference model. [Layer (N) has boundaries to layer (N + 1) and to layer (N − 1).]

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

5GC Fifth Generation Core network

AAA Authentication, Authorization and Accounting

AMF Access and Mobility management Function

BGP Border Gateway Protocol

BNG Broadband Network Gateway

CDN Content Delivery Network

CGNAT Carrier Grade Network Address Translation

CPU	Central Processing Unit
CS	Circuit Switched (domain)
DCN	Data Communication Network
DRA	Diameter Routing Agent
FRR	Fast Reroute
HSS	Home Subscriber Server
IGP	Internal Gateway Protocol
IGW	Internet Gateway
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
LAG	Link Aggregation
LFA	Loop-Free Alternate
LTE	Long-Term Evolution
MLAG	Multichassis Link Aggregation
MME	Mobility Management Entity
MPLS	Multiprotocol Label Switching
NE	Network Element
NMS	Network Management System
OOB	Out-of-Band
OSPF	Open Shortest Path First
OTT	Over-The-Top
P	Provider
PCRF	Policy and Charging Rules Function
PE	Provider Edge Router
PGW	Packet Data Network Gateway
Pre-agg	Pre-aggregation
PS	Packet Switched (domain)
RAT	Radio Access Technology
RR	Route Reflector
SGW	Serving Gateway
SLA	Service Level Agreement
ToB	To Business
ToC	To Customer
UDM	Unified Data Management
UPF	User Plane Function
VNF	Virtual Network Function

VPN Virtual Private Network

5 Introduction

5.1 Background

The concept of resilience originated in physics, denoting a material's capacity to return to its original state following disturbance. As cyber threats have escalated in sophistication and scale, nations have systematically integrated resilience into systems engineering, information technology and computer networks, and have elevated network resilience to a key direction of their national strategies.

- In 2013, the United States issued Presidential policy directive 21: Critical infrastructure security and resilience 0, which formally defined network resilience for the first time. In 2021, the National Institute of Standards and Technology (NIST) released Developing Cyber-Resilient Systems: A Systems Security Engineering Approach 0, proposing a comprehensive engineering framework for network resilience. This framework has become guidance for the US Government's network resilience efforts and a cornerstone for global resilience research.
- The European Union's Cyber Resilience Act officially entered into force in December 2024, requiring all digital technology products entering the EU market to possess high network resilience 0.
- The China IMT-2030 (6G) Promotion Group released White Paper on 6G Network Architecture Vision and Key Technology Outlook, explicitly identifying resilience as one of the key design principles for future network architectures **Error! Reference source not found.**.
- In 2022, the UK Government published the National Cyber Strategy 2022, emphasizing network resilience as a key pillar and identifying "security and resilience" as one of the four core national cyber strategy objectives 0.
- Japan's Ministry of Internal Affairs and Communications (MIC) released a B5G development strategy that outlines a social vision for 2030 centred on dependability, inclusiveness and sustainability, stating that B5G must feature ultrasecurity and resilience 0.

Current network resilience efforts primarily focus on discrete technical modules such as network attack and defence, emergency response and disaster recovery redundancy, lacking a systematic perspective. For future network resilience, attention must extend beyond technological innovations to encompass holistic strategies and cross-domain collaboration. This Technical Report sorts out typical use cases of future network resilience, extracts universal resilience requirements and provides practical support for the systematic construction and capability architecture optimization of network resilience.

5.2 General concept of future network resilience

Network resilience refers to the capability of a network to continue to perform its intended functions correctly during and after natural or human-made disturbances, and to provide and maintain an acceptable level of service in the presence of various faults, attacks or other adverse conditions. Network resilience focuses not only on fault prevention, but also on sustaining service continuity, limiting performance degradation, enabling timely recovery and supporting long-term evolution in response to changing network environments.

This Technical Report adopts a lifecycle-based approach to describe network resilience, in which resilience objectives are organized into four interrelated stages: anticipate, withstand, recover and adapt. These stages represent both temporal phases and functional objectives, as illustrated in Figure 1.

a) Anticipate: Maintain a state of informed preparedness for adversity;

b) Withstand: Continue essential mission or business functions despite adversity;

c) Recover: Restore mission or business functions during and after adversity;

d) Adapt: Modify mission or business functions and/or supporting capabilities in response to predicted changes in the network architecture, network topology, traffic pattern and so on.

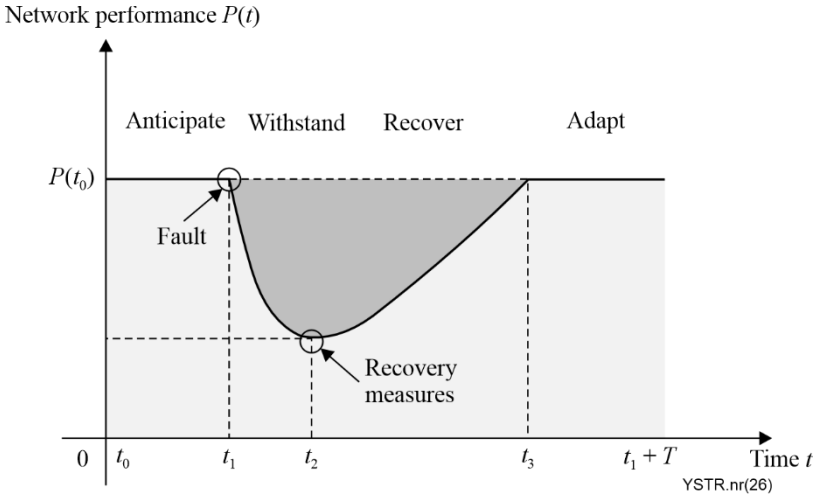


Figure 1 – Quantitative definition of future network resilience

This Technical Report follows the network resilience objectives to define future network resilience use cases, capabilities and objectives in terms of network infrastructure, NEs, network protocols, network design and service impact.

As shown in Figure 2, future networks are facing a trend of rapidly increasing scale and complexity. Therefore, it is necessary to analyse the key elements of network resilience at various layers of the network.

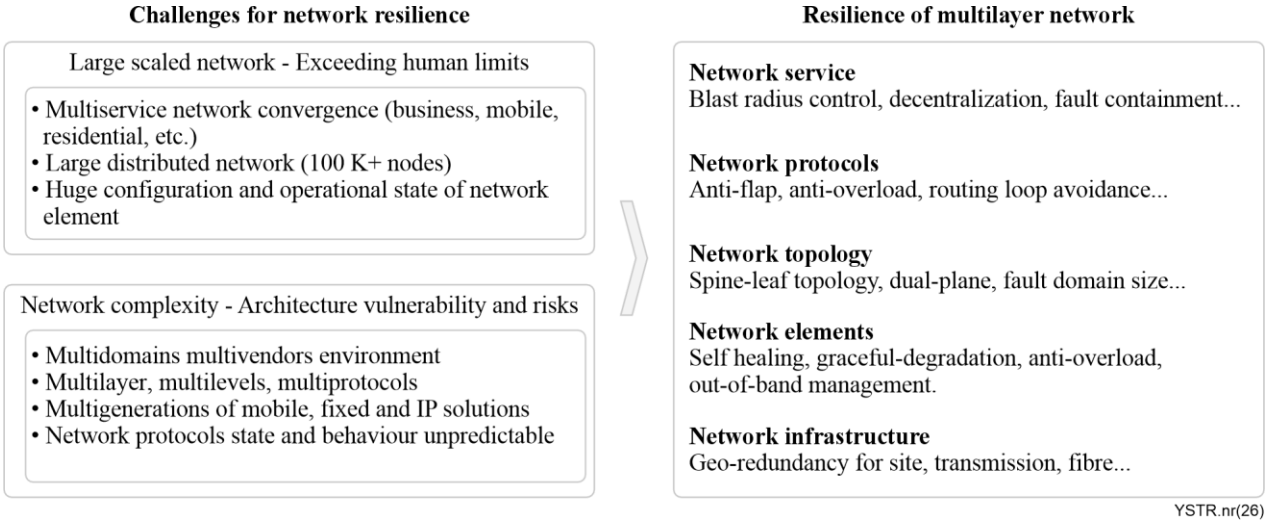


Figure 2 – Network resilience challenges and considerations

The future network resilience refers to the capability of maintaining the functions and performance with acceptable SLA level, when it encounters various possible faults, attacks or other faults. The network resilience can be improved through multiple approaches, i.e., redundancy backup, distributed architecture, traffic engineering and policy, routing fast reroute to improve the anti-attack capability, fault isolation capability, fast recovery capability of the network to ensure the network safety and service continuity.

6 Generic consideration of future network resilience

Based on the resilience lifecycle, future network resilience can be systematically characterized through a set of generic capability considerations. The four resilience phases – anticipate, withstand, recover and adapt – represent different objectives over the lifecycle of adverse events, from proactive preparedness to long-term evolution. These phases are supported by various capabilities of the network.

The anticipate phase is primarily supported by network fault prevention capability and network awareness capability, which enable proactive risk mitigation and early detection of abnormal conditions. The withstand phase is mainly supported by network fault tolerance capability and network fault containment capability, which aim to absorb faults, maintain essential services and limit fault propagation during adverse events. The recover phase is supported by network recovery capability, which enables efficient restoration of network functions and service performance. The adapt phase is supported by network resilience re-architect capability, which enables the network to evolve and enhance its resilience in response to historical incidents and future risks. Together, these capability considerations form an integrated framework that supports end-to-end network resilience across infrastructure, network elements, protocols, topology and services.

The following subclauses describe each generic capability consideration in detail.

6.1 Network fault prevention capability

Network fault prevention capability refers to the consideration that the network architecture and specific design should be preventive and proactive, to avoid network accidents or adopt response strategies when abnormal network events occur. This capability applies across the infrastructure layer, network element layer, network layer and service layer.

6.2 Network awareness capability

Network awareness capability is the basic common capability. The network should have the ability to perceive network status and detect abnormal events across the multi-dimension consisting of the infrastructure layer, network element layer, link layer, protocol layer, VPN layer and service layer. It should be aware of the various network states including but not limited to configuration status, network protocols status, forwarding path status of the data plane and service performance status. It should support the ability to detect abnormal conditions, events or behaviours, and take appropriate countermeasures.

NOTE – In the context of this Technical Report, an Abnormal Event refers to any unexpected or irregular faults that could affect network operational status or performance, which could be routing flaps, IP addresses or Router ID conflict or protocol bugs, etc.

6.3 Network fault tolerance capability

Network fault tolerance capability refers to the consideration that the network should support redundant backup, remote disaster recovery and other solutions to deal with abnormal events or module failures in the network. For the network layer of the multilayer network architecture, the network should support redundancy and diversity from local protection, which safeguards local facilities against local link or directly connected neighbouring node failures, to path protection with different granularities; the redundant protection deployed in each layer of the network should support cross-layer and cross-domain protection collaboration to filter and absorb abnormal events occurring in the lower layers.

6.4 Network fault containment capability

Network fault containment capability refers to limiting the scope of fault impact, isolating fault events, reducing the fault domain or blast radius, and controlling the scope of fault diffusion. When an abnormal event occurs in a particular module in the network, the abnormal event will be further

transmitted and propagated multi-dimensionally to the associated modules. In extreme scenarios it will trigger an avalanche effect with a wider range. In order to limit the spread of such events and avoid a critical impact, each component in the network should have the ability to isolate and contain abnormal fault events.

NOTE – In the context of this Technical Report, the blast radius refers to the scope or extent of impact on users, services, network elements, links and protocols following a fault or failure event.

6.5 Network recovery capability

Network recovery capability refers to the restoration of the network to its original normal state in case of an abnormal event. This capability includes: network fault and failure detection, locating, diagnosing and recovering; network recovery management process with team collaboration, workflow and process design, emergency plans and resource preparation; and network elements out-of-band access management and control capabilities, etc.

6.6 Network resilience re-architect capability

Network resilience re-architect capability refers to the mid-term and long-term proactive resilience planning for future risk challenges. These challenges need to be clearly identified to cover major historical risks and future potential risks. The mid-term or long-term resilience architecture should include the countermeasures to address those future risks. Furthermore, both the future risk challenges and the resilience architect plan need to be evaluated routinely.

7 Use cases and root cause analysis

This clause will provide future network resilience use cases with analyses: Network architecture risk, abnormal traffic pattern, routing loops, hardware or software failure, malicious attack, etc.

7.1 Use Case 1: Inaccurate network planning and design deficiency

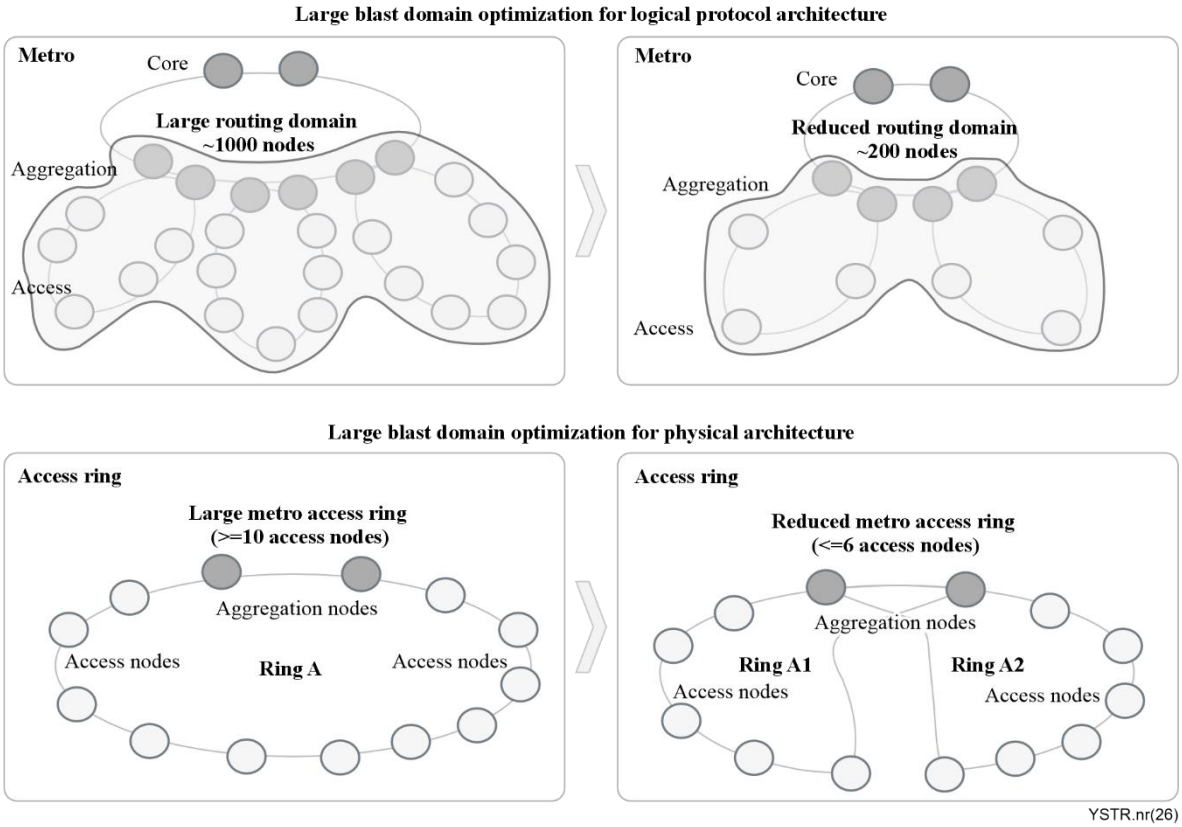


Figure 3 – Large blast radius domain reduction

With the continuous growth of network scale and complexity, network planning and designing play a critical role in overall resilience. In large-scale networks, a single routing domain may include thousands of nodes and metro access networks may adopt large ring topologies.

As illustrated in Figure 3, an oversized routing domain or access ring leads to a large blast radius. In such scenarios, incidents caused by misconfiguration, mis-operation or protocol defects (e.g., routing loops or control-plane overload) may result in widespread service impact. In addition, excessive hop count may increase end-to-end latency and degrade service experience.

The root causes include insufficient fault domain partitioning, lack of blast radius control and absence of automated planning rules. This use case highlights the need for network fault prevention capability and fault containment capability, supported by optimized topology design and automated planning mechanisms.

7.2 Use Case 2: Impairment of routing integrity and stability

The IP routing is the key component for future network and the routing status directly impacts the network stability and availability. When the routing stability degrades, service SLA will degrade as well.

As shown in Figure 4, because of routing policy misconfiguration on aggregation nodes, the aggregation node prefers the routes from other aggregation nodes and sends them back to the metro core. While the metro core prefers the routes from aggregation to the one learned from the IP core, routing loops are formed.

When links between the metro core node and IP core are activated, the mobile service routes from IP core experience routing loops between metro core and aggregation nodes, and thus all mobile services experience outage.

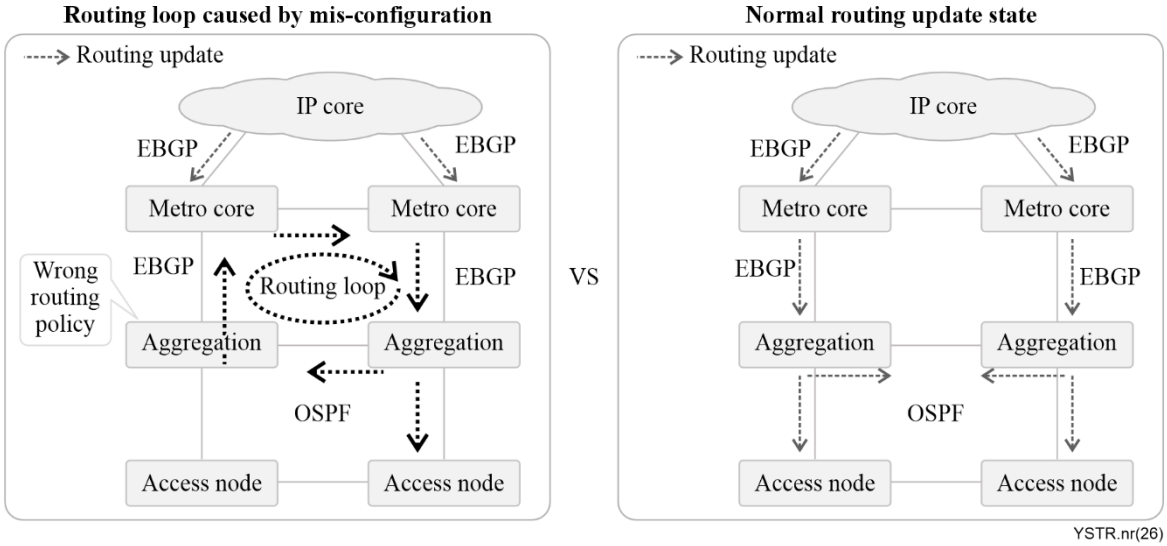


Figure 4 – Routing protocols loop

Typical root causes include improper route redistribution between routing protocols, missing or incorrect routing policies, and topology or design changes affecting best-path selection. This use case emphasizes the importance of network prevention capability to avoid incorrect routing policy and network awareness capability for detecting abnormal routing behaviour.

7.3 Use Case 3: Router resource exhaustion and control-plane overload

Network overload may occur in multiple dimensions, including device CPU, memory, protocol databases and routing tables. In extreme cases, overload may lead to device restart or crash.

Network expansion and scale as service grows could be one cause for overload, in this case, there are increasing links, devices, routes which will hit the limit for a particular network module if the capacity is not well designed or protected. Figure 5 below shows two network outage accident cases caused by BGP and IGP routes overload. In Case A, BGP speakers have no corresponding policy configuration, when massive routes flood from the Internet to the network, PE1 and PE2 BGP are overloaded. In Case B, there are two scenarios of IGP OSPF routes overload, PE1 routes overload when importing large BGP routes into OSPF; PE2 routes overload by OSPF flooding within the OSPF domain.

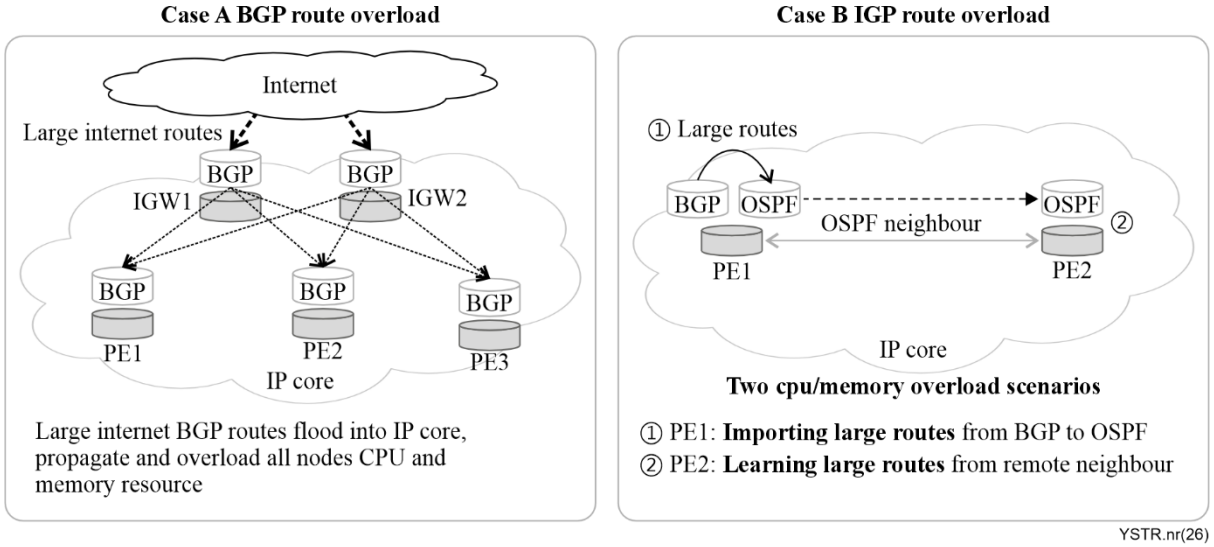


Figure 5 – BGP and IGP/OSPF route overload

The root causes include insufficient capacity planning, lack of route admission control, and absence of overload protection mechanisms. This use case demonstrates the need for fault tolerance capability and fault prevention capability, including graceful degradation, route limiting and resilient routing design.

7.4 Use Case 4: Network flapping events

Flapping events, such as link flaps, protocol neighbour flaps or route flaps, are common operational challenges and may significantly impact network stability.

As shown in Figure 6, because the "interface dampening" configuration is not enabled on PE1 and P1 to filter link flap events, when the link between PE1 and P1 flaps, the interface of the link, routing protocols and service routes start to flap as well, and the left part of the mobile service experiences quality degradation.

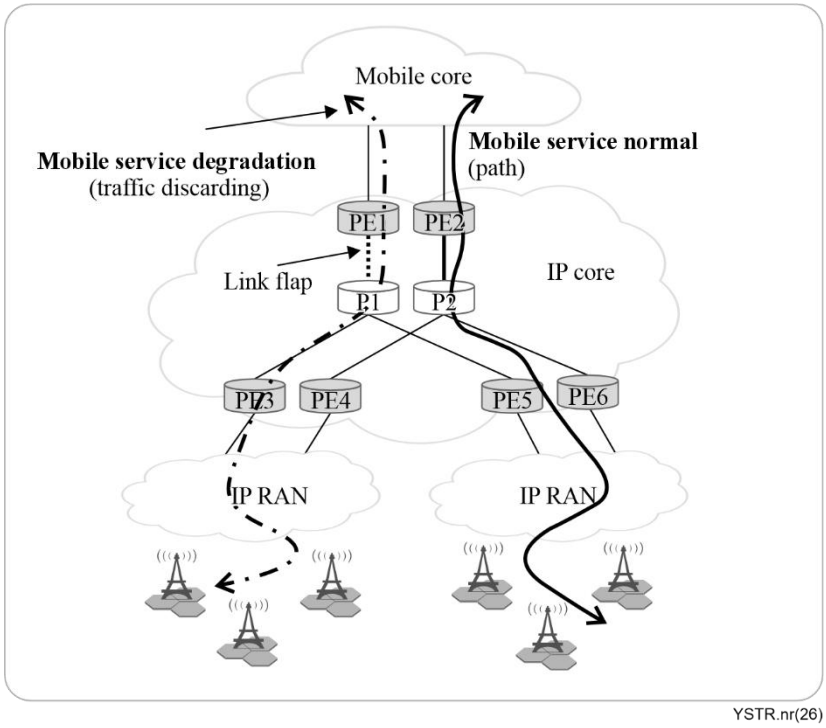


Figure 6 – Link flaps cause service degradation

The link flaps could be triggered by other causes such as an unstable transmission network and interface optical module deterioration. To mitigate the impact of link, protocols, routes or other flap events, the network devices should deploy various dampening mechanisms to handle those events. The device starts to react for fast convergence when detecting the link, protocols, routes status changes for the first time, but suppress and filter the events when the status continues to frequently change between up and down. This use case highlights the need for fault tolerance capability and fault containment capability.

7.5 Use Case 5: Always-on network management

When the device crashes due to issues, the operators arrange engineers on-site to restore the device back to a working state. To restore the device back to service as soon as possible, the high resilience solution is to have the device "always on" to shorten the duration for recovery activity, which means the operator can log in and configure the device remotely at any time.

As illustrated in Figure 7, the service network is on the left, a dedicated OOB DCN for management is in the centre and the NMS platform is on the right. Since the DCN is isolated from the service network, administrators can still access network elements through the DCN for out-of-band troubleshooting and recovery even if the primary service network fails.

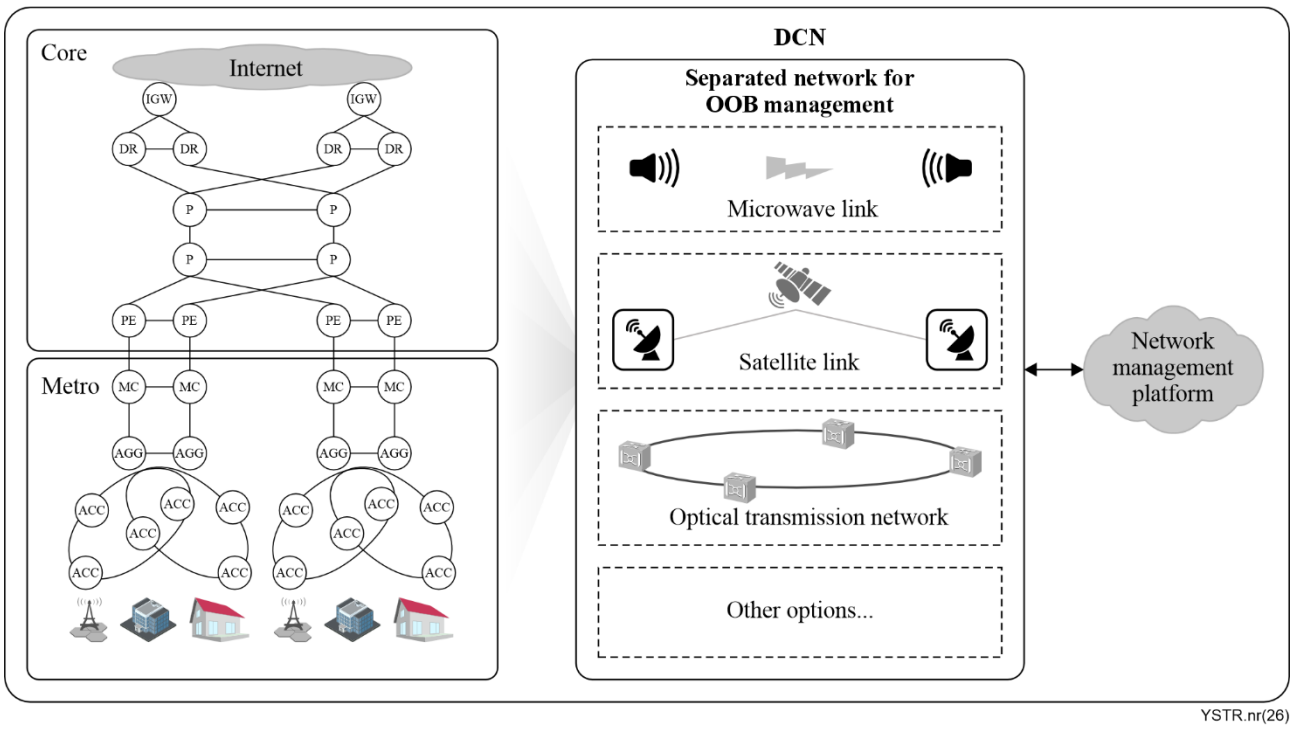


Figure 7 – Isolated network for OOB network management

This use case demonstrates the importance of network prevention and recovery capability. To achieve devices "always on", the network and devices could provide multiplane isolation capability. The management plane, control plane and forwarding plane of the device should be isolated from each other to avoid coupling issues, such as abnormal routing protocol update bursts or forwarding failure messages overwhelm the management channel.

There are some other approaches to keep the devices in service with high resilience network planning and preparation capability, to ensure the devices could be connected anytime, such as building necessary redundant links, enable local management accounts in case AAA servers fail and seting up out-of-band connection for device management.

7.6 Use Case 6: Mitigation of signalling storms and snowball effects

Network operations or network element failures cause service interruptions, leading to repeated automatic retries by the terminal. During the terminal's retry process, the core network service elements gradually become overloaded, triggering a "snowball" effect, which in turn generates a signalling storm, dramatically amplifying the impact of the incident.

When a signalling storm occurs, core network elements can take flow control to avoid overload, while also protecting subsequent signalling processing elements from significant impact, thereby preventing the further amplification of the effects.

As shown in Figure 8, different flow control capabilities are deployed across the four domains of PS/5GC, CS/IMS, signalling transfer point and data domain, thereby mitigating the impact of signalling storms. The flow control mechanism deployed in the four domains consists of four defence lines. There are three types of flow control deployed:

1. Access flow control: set the flow control threshold for incoming messages based on the NE processing capability.
2. Self-insurance flow control: the system discards incoming messages to ensure that the system does not break down.

3. Protecting third parties: set the flow control threshold based on the peer NE capability or the flow success rate.

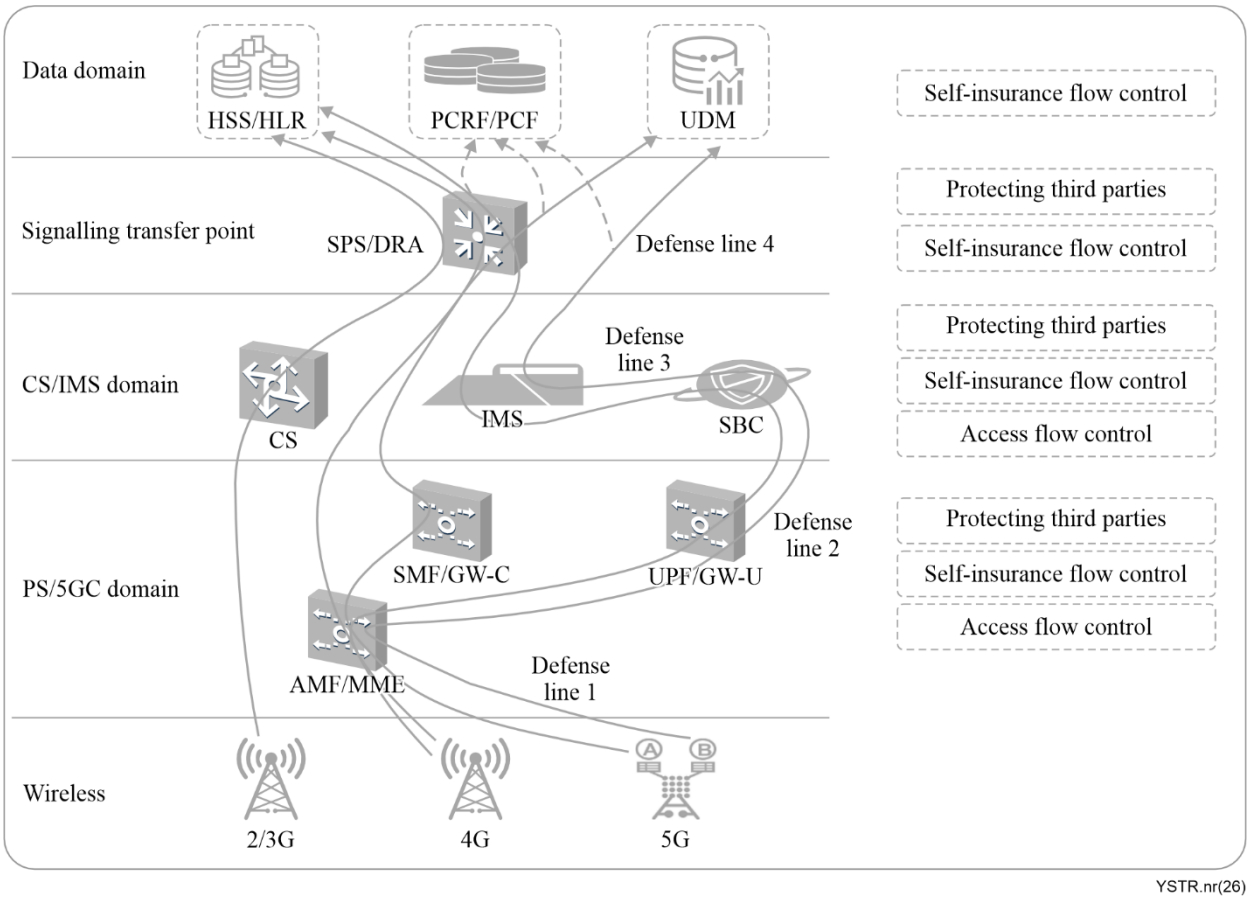


Figure 8 – Typical core network four lines of defence of flow control

In addition, mobile core network elements such as AMF/MME can deploy hot backup mechanisms, as shown in Figure 9, to reduce additional signalling interactions during failures and prevent further signalling amplification.

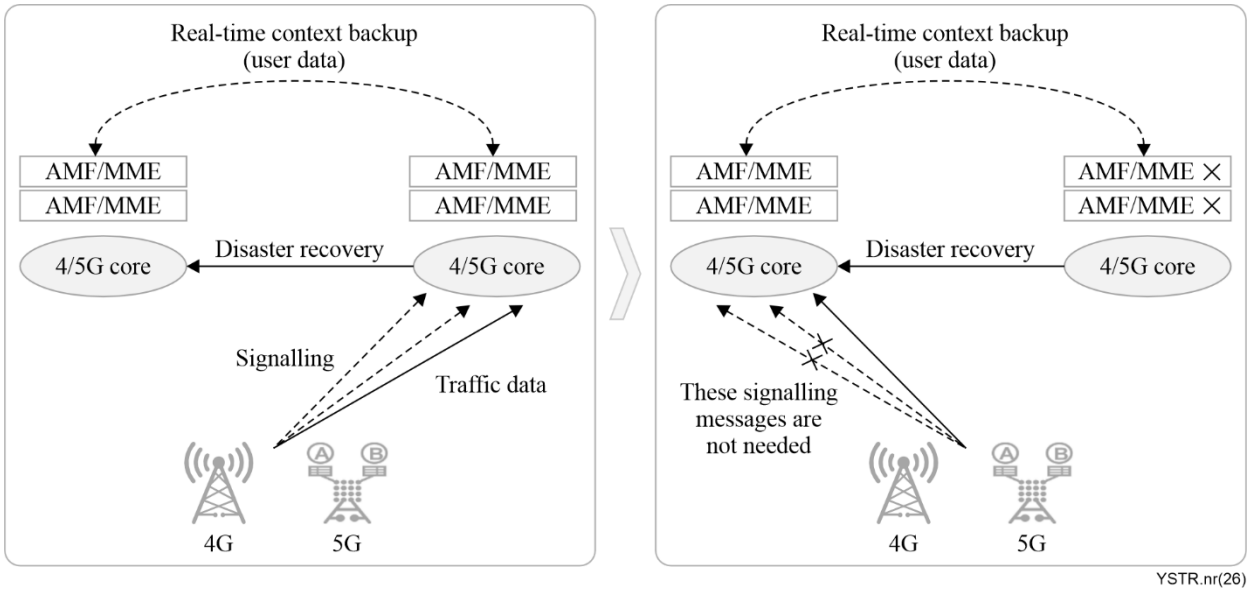


Figure 9 – Typical core network AMF/MME hot backup

This use case mainly requires network fault prevention capability to limit signalling propagation, network fault tolerance capability to maintain service continuity, and network awareness capability to detect abnormal signalling behaviours.

7.7 Use Case 7: Regional service self-containment

The inappropriate deployment locations of core NEs may increase the potential risks. As shown in Figure 10 (left), there are four mobile areas in the network. User information storage devices (UDM/HSS or PCRF) and DRA are both deployed in the central area. Data and voice services located in the edge areas need to access these devices in the central area. This architecture creates a vulnerability: any transmission failure between the central and edge regions triggers service outages at the edge.

To mitigate this, a distributed deployment is essential. By localizing user data and signalling functions within each region, services can operate in a "closed-loop" manner, ensuring robust fault containment and fault tolerance.

This use case demonstrates the need for fault tolerance capability and fault containment capability.

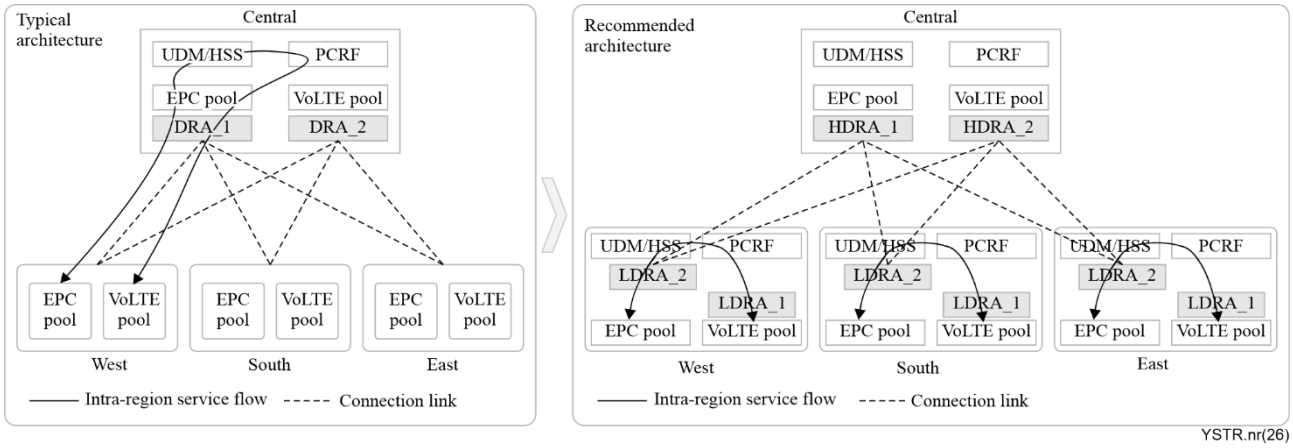


Figure 10 – Typical core network topology

7.8 Use Case 8: Over-centralized network element deployment

Over-centralized NE deployment may cause numerous issues; when transmission failures, power/air conditioning outages or natural disasters happen in this site, there might not be enough remaining NEs to sustain services.

As shown in Figure 11, the number of VNFs in "Resource pool1" and "Resource pool2" are unbalanced. If "Resource pool1" is faulty, it will impact three VNF services and VNF4 may not have enough capacity to take over these services. It is recommended to relocate one VNF3 to "Resource pool2" to achieve load balancing.

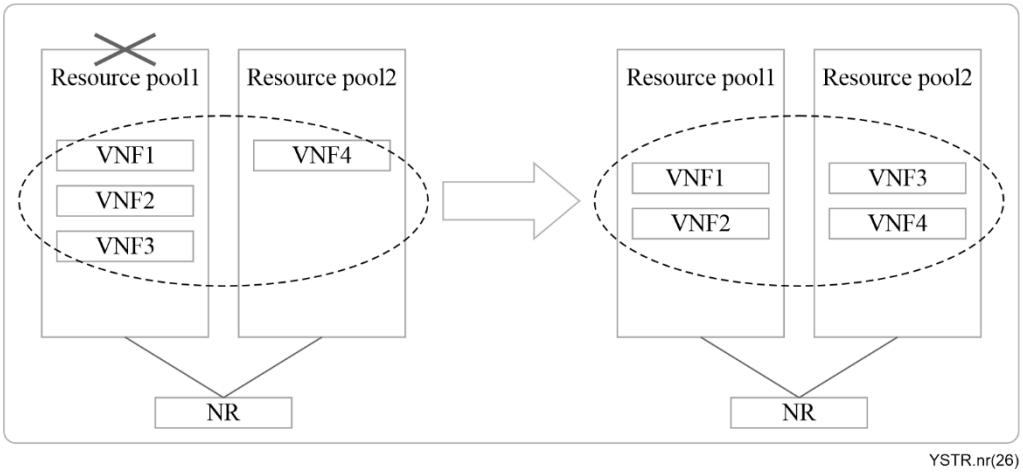


Figure 11 – Core network VNF distribution design

Similar incidents have occurred in operational networks, such as power failures at sites hosting a majority of network capacity or centralized HSS deployment causing nationwide service outages. These incidents are primarily caused by insufficient deployment dispersion and a lack of geographical redundancy.

To mitigate such risks, network elements should be deployed across diverse data centres and geographical locations. This use case highlights the need for network fault tolerance capability and network resilience re-architect capability to optimize network deployment and improve long-term resilience.

7.9 Use Case 9: Network resilience evaluation and re-architecting

Future networks continuously evolve due to traffic growth, service introduction, software upgrades and architectural changes. These changes may introduce new risks, such as dirty traffic injection, protocol bugs or routing anomalies.

Operational experience shows that without continuous evaluation and refinement, networks may gradually become fragile and unstable. The root causes include inadequate risk assessment, deficient resilience validation and suboptimal architectural adaptation.

This use case highlights the importance of network resilience re-architect capability, enabling continuous assessment, optimization and evolution of network architecture based on historical incidents and future risks.

8 Specific consideration of future network resilience

This clause translates the observed challenges and failure patterns into concrete technical capability considerations for future network resilience. The focus is placed on architectural, protocol and operational capabilities that enable networks to anticipate, withstand, recover from and adapt to adverse events. These capability considerations provide technical guidance for network planning, design, and evolution and serve as a foundation for the resilience architecture and best practices discussed in clause 9.

8.1 Logical routing architecture redundancy and diversity capability

As a logical layer of the network architecture consisting of several sublayers including the IGP layer, IP/MPLS tunnels layer and VPN layer, the routing layer shall support various redundancy technologies and diversity between the redundant modules to protect from fate-sharing risk. Each routing protocol component is expected to provide end-to-end or local protection against link and node failures across the network, such as FRR or LFA mechanisms in IGP and BGP. At the service

level, multihomed network access should be supported to avoid single points of failure, operating in either load-balancing or primary/backup modes. Key network services should be delivered over multiple logical service paths traversing different devices and forwarding planes, so that service continuity can be maintained when individual nodes or links fail. In addition, routing redundancy should incorporate diversity in terms of paths, locations and underlying infrastructure resources to avoid shared risks.

8.2 Physical network architecture redundancy capability

Physical network architecture redundancy should support redundancy at component, network element and service levels, while critical network elements should additionally support geographical redundancy. Network devices with high redundancy capabilities are recommended, including modular platforms with full redundancy for power, cooling, fabric and control components, as well as fixed-configuration devices with essential component redundancy. Key network elements such as PE and BNG, together with their interconnection links, should be deployed in redundant configurations using load balancing or primary/backup mechanisms, with link-level redundancy supported by technologies such as link aggregation (LAG) or multichassis link aggregation (MLAG). For network elements handling dynamic user data, real-time data synchronization between redundant elements is required to prevent signalling storms during failover scenarios. Furthermore, critical network elements should be geographically distributed across different sites to ensure resilience against site-level failures.

8.3 Service, routes, traffic and device anti-overload capability

Service, routing, traffic and devices overload can consume and exhaust network resources leading to service and network performance degradation or critical outage. Therefore, the network architecture should incorporate comprehensive anti-overload mechanisms. Service NEs should be able to control and prioritize different types of messages under overload conditions, based on their service importance and system impact, while dynamically adapting traffic volumes according to downstream congestion states. The routing architecture should include anti-overload policies such as routing filters and prefix limits for both overlay and underlay protocols. Traffic management mechanisms should support classification, rate limiting, abnormal traffic detection and capacity dimensioning to mitigate risks arising from traffic surges or topology changes. In addition, the network architecture shall adopt the devices with anti-overload capability, which can decrease route learning rate by observing resource (e.g., CPU, memory) consumption.

8.4 Network topology awareness capability

Future networks typically consist of vertically layered physical and logical topologies. To improve overall resilience, the network management platform should maintain comprehensive awareness of these topologies. This includes physical topology, Layer 2 and Layer 3 topologies, underlay IGP/MPLS topology, overlay VPN topology and IP/MPLS forwarding paths. The management platform should support visualization of mobile core network topologies, including interface relationships, disaster recovery associations and traffic forwarding paths. Topology information should be updated dynamically in response to network changes, and the platform should provide situational awareness by correlating historical topology states with current conditions and future trends.

8.5 Network performance awareness capability

The network management platform maintains continuous awareness of both real-time and historical network and service performance. This includes performance indicators such as latency, jitter and packet loss at link, path and service levels. Performance data should be visualized through topology-based views, including latency or congestion maps, and extended to upper-layer services including

voice and data services. In addition to real-time monitoring, the management platform should support performance trend analysis and predictive awareness to enable proactive resilience management.

8.6 Cross-domain network resilience capability

Resilience design across mobile core, IP bearer and transmission domains should support protection coordination, blast radius containment and fault demarcation. Lower-layer network domains should provide isolated nodes and links to support redundant paths for upper-layer services. Network elements in upper domains should be distributed across diverse facilities in lower domains to reduce the impact on lower-layer failures. Furthermore, cross-domain management systems should support fault detection and demarcation across domains, enabling rapid localization of faults affecting service traffic.

8.7 Survival capability

In extreme scenarios, the network and services should support survival capabilities that enable service continuity or graceful degradation. Key services may adopt multiple design approaches, such as dual independent planes or additional backup paths that serve as a last-resort mechanism when primary and secondary components fail. Core network elements should support bypass mechanisms so that essential voice and data services can be maintained even when specific functional nodes fail. In addition, service resilience mechanisms should support inter-RAT fallback, allowing user equipment to access alternative radio access technologies when higher-generation networks are unavailable. Network elements should be capable of remaining operational with minimal functionality and support out-of-band management to enable recovery under severe conditions.

8.8 Blast radius optimization capability

Blast radius optimization ensures that the network and devices can absorb and isolate abnormal events to limit the impact. This capability mainly applies to the topology architecture design. At the network element level, service density per device should be controlled, and the scale of resource pools should be optimized to reduce the impact of failures. At the topology level, protocol domains such as Layer 2 flooding domains, IGP areas and BGP RR clusters, which collaborate via route reflectors and clients to distribute routing, should be dimensioned to prevent cascading failures. For critical network positions, multiplane architecture designs may be adopted to contain service impact within individual planes. At the service layer, core network elements should be distributed across multiple facilities to reduce user impact during events such as data centre outages or transmission interruptions.

8.9 Service and network separation capability

To reduce complexity and dependency risks, service and network layers should be logically and physically separated where feasible. At the network element level, devices with specific functional roles should separate underlay forwarding from service functions, including RR nodes, core P nodes and metro aggregation and core nodes. The network layer should remain largely service-agnostic, with minimal dependencies on service-layer logic. At the service layer, the number of service-network interaction points should be minimized and placed closer to the network edge. For enhanced resilience in core network architectures, to business (ToB) and to Customer (ToC) services should access physically isolated network elements.

8.10 Key network nodes and service distribution

Services and the key network nodes supporting them should be geographically distributed to reduce the blast radius and improve quality of experience. Fixed services and related network elements such as BNG, PE and CGNAT should be deployed close to residential and enterprise users. Mobile services and associated core nodes, including UPF, SGW and PGW, should be deployed closer to radio access networks. Internet services and CDN components should be distributed from IP core networks towards metro networks to improve resilience and performance.

8.11 Hierarchical and modular design, clean network architecture

The network shall have a clean architecture with regular topology. Across metro access, metro aggregation, metro core and IP core networks, each layer should have a clearly defined role and avoid functional overlap. In IP core networks, P and PE nodes should have strictly separated functions, with P nodes providing aggregation and PE nodes serving as service edges. Metro networks should connect directly to the IP core and remain where each node is dedicated to a specific function mutually isolated, while maintaining clearly separated functions among the access, aggregation and core layers within each metro network.

8.12 Logical layered protocols architecture

Protocols deployment shall adopt a layered and modular architecture and adopt and comply with the principles of hierarchy, regionalization and service orientation. This applies to logical layer protocols IGP, BGP, etc. Large-scale IGP domains should adopt hierarchical designs with core and access areas, while different metro networks or regions should use separate IGP domains to limit fault propagation. Critical services may use dedicated IGP domains to improve resilience. BGP route reflectors (RRs) should be deployed hierarchically with separate clusters aligned to network levels, regions and services, thereby preventing fault diffusion across regions or service domains.

9 Best practice of future network resilience architecture

Figure 12 illustrates the target architecture of future network resilience, which leverages multiple considerations of future network resilience. The following clauses will explain the detailed design implementations.

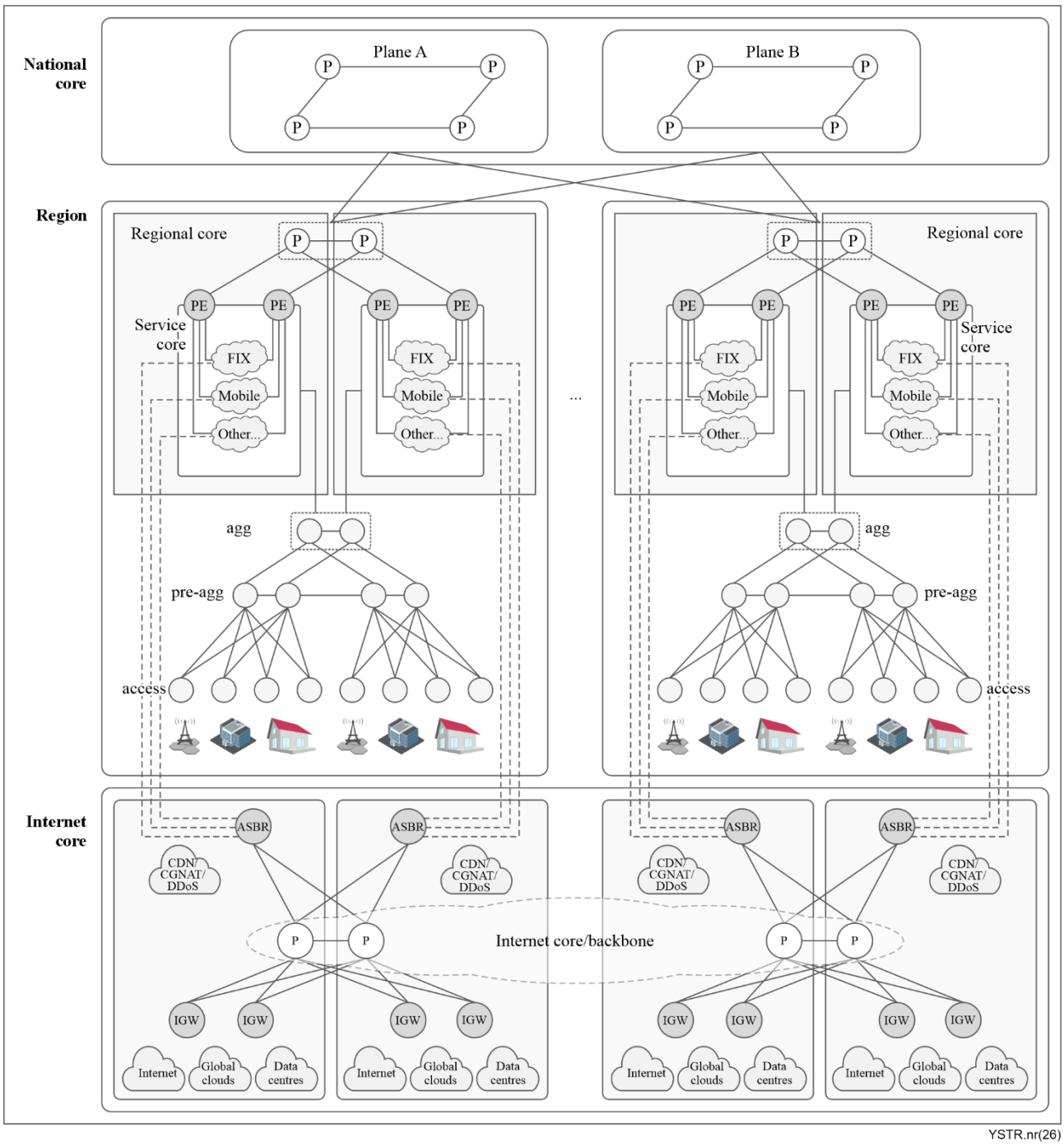


Figure 12 – Target architecture of future network resilience

9.1 Distributed service architecture

The specific considerations defined in clauses 8.9 and 8.10 are used here.

As shown in Figure 12, all services – including fixed-line, mobile, and Internet/OTT content – have been transitioned from the national core to a distributed service architecture across individual regions. Specifically, fixed-line, mobile, and enterprise services are now localized at the regional core, with each region deploying two sites for geo-redundancy. Meanwhile, Internet, CDN and OTT services are deployed at the regional level within a dedicated Internet core domain, and are often co-located with other regional services. This decentralized architecture effectively eliminates network-level outages and minimizes the blast radius. Even in the event of an IP core failure, regional services remain operational, ensuring business continuity.

9.2 Independent Internet core with regionalized Internet contents

The specific considerations defined in clauses 8.3, 8.8 and 8.9 are used here.

IGWs for Internet, CDN, and OTT access are deployed within a separate Internet core network, which exclusively provides Internet-relevant services. The Internet core's footprint extends across all regions, typically with at least two sites per region for resilience. Each site hosts a combination of CDN caches, domestic IGWs and international IGWs. All upstream providers, peering partners and downstream customers connect at these regional sites. This independent IGW network effectively isolates Internet/BGP-related risks and incidents, thereby safeguarding the internal regional and national core networks.

9.3 Vendor diverse dual-plane national core

The specific considerations defined in clauses 8.1, 8.2, 8.8 and 8.9 are used here.

The national core utilizes a dual-plane architecture, comprising two active-parallel planes (referred to as Plane A and Plane B) that provide mutual redundancy. These planes are physically isolated from one another, with each plane using equipment from a different vendor to mitigate vendor-specific technology vulnerabilities. In the extreme event of a single-plane failure caused by vendor-specific hardware or software defects, the national core architecture ensures resilience and business continuity via the surviving backup plane.

9.4 Isolated network design principle to optimize Blast Radius

The specific considerations defined in clauses 8.8, 8.10, 8.11 and 8.12 are used here.

The architecture is designed with three isolated core tiers: a national core, regional cores and an Internet core, each operating over physically/logically isolated transmission networks. The network is further segmented into several autonomous regions, which are isolated from one another. To enforce manageability and contain failures, specific design constraints are applied: the region access ring network size is dimensioned for a maximum of six nodes and the IS-IS protocol domain for regional access networks is strictly limited to a maximum of 200 nodes.

This isolation strategy effectively controls the blast radius for various failure scenarios:

- A failure in one core tier (e.g., Internet core) ensures the continued operation of the other two (national and regional).
- An outage in one region is contained, preventing impact to the remaining other regions.
- Maximum size limits constrain any failure domain to a maximum of six nodes within an access ring or 200 nodes within an IS-IS domain.

9.5 Geo-redundancy and diversity for key services and nodes

The specific considerations defined in clauses 8.2, 8.6, 8.8 are used here.

By deploying Regional Cores with dual sites in distinct geographic locations, mobile, enterprise and fixed-line services achieve full geo-redundancy. Within each region, nodes providing mutual backup for the national, regional, and Internet cores are geographically dispersed to ensure site-level disaster recovery.

Furthermore, all sites are supported by robust fibre infrastructure, featuring triple-homed or multi-directional diverse fibre paths (at least three independent routes). This geo-redundant architecture ensures that service continuity is maintained even in the event of a total site or regional core failure.

Bibliography

[b-ITU-T Q.1290] Recommendation ITU-T Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks.*

[b-ITU-T Y.1231] Recommendation ITU-T Y.1231 (2000), *IP Access Network Architecture.*

[b-ITU-T Y.1714] Recommendation ITU-T Y.1714 (2009), *MPLS management and OAM framework.*

[b-EU] European Union (2024), *Cyber Resilience Act,* 202270272(COD).
https://data.consilium.europa.eu/doc/document/PE-100-2023-INIT/en/pdf

[b-IMT-2030] IMT-2030 (6G) Promotion Group (2021), *White Paper on 6G Network Architecture Vision and Key Technology Outlook*
https://www.caict.ac.cn/english/news/202106/P020210608349616163475.pdf/

[b-Ross] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., and McQuaid, R. (2021), *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, US National Institute of Standards and Technology.
https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

[b-UK Government] United Kingdom Government (2021), *National Cyber Strategy 2022*.
https://www.gov.uk/government/publications/national-cyber-strategy-2022

[b-White House] White House (2014), *Presidential policy Directive 21: Critical infrastructure security and resilience*
https://www.researchgate.net/publication/293071200_Presidential_policy_directive_21_Critical_infrastructure_security_and_resilience

[b-XGMF] XG Mobile Promotion Forum (2025), *Beyond 5G White Paper*
https://xgmf.jp/wp-content/uploads/2025/04/Beyond_5G_White_Paper_v4_0.pdf