ICS 35.240.01
CCS L04

团　体　标　准

T/ZGTXXH 072—2023

算网融合 网络基础设施 IP 网络韧性规范

IP Network resilience specification for computing network convergence network infrastructure

2023-06-20 发布　　2023-06-20 实施

中国通信学会　　发 布

目　　次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 1
5 算网融合 IP 网络韧性概述 2
6 算网融合 IP 网络韧性的分级和目标 3
6.1 IP 网络韧性分级 3
6.2 IP 网络韧性目标 4
7 算网融合 IP 网络韧性能力评估 5
7.1 IP 网络韧性评估目标 5
7.2 IP 网络韧性评估要求 5
7.3 IP 网络韧性评估总体框架 5
7.3.1 IP 网络韧性评估指标体系 6
7.3.1.1 量化评测项 6
7.3.1.2 量化评分项 7
7.3.1.3 IP 网络韧性总分数 8
7.4 IP 网络韧性能力评估方法 8
7.4.1 评估方法总览 8
7.4.2 扰动库构建 9
7.4.3 业务流构建 10
8 算网融合 IP 网络韧性能力要求 11
8.1 总体要求 11
8.2 网元韧性能力要求 11
8.3 网络级韧性能力要求 12
8.3.1 冗余多样规划 12
8.3.2 故障隔离规划 12
8.4 业务级 IP 网络韧性能力要求 12
8.5 运维级韧性能力要求 13
8.5.1 网络管理规划 13
8.5.2 故障恢复规划 13
8.5.3 操作容错规划 13

前　言

本文件依据GB/T1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国通信学会提出并归口。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件起草单位：中国信息通信研究院、华为技术有限公司、中国联通研究院、中国电信股份有限公司研究院、中国科学院计算机网络信息中心、中国移动研究院。

本文件主要起草人：韩淑君、周宇、穆琋博、顾月峰、茅利、刘剑南、张超、行骁程、柴瑶琳、李建飞、李云鹤、申罕骥、姚惠娟。

本文件为首次发布。

引　言

近年来全球不断出现重大的IP网络事故，对终端用户、ICT服务提供商和设备提供商都造成了非常恶劣的影响。在IP网络可靠性和业务可用性的基础上，需要构建高韧性的网络，在网络故障和错误操作出现时，能够控制故障影响范围，并及时引入防冲击机制，明确逃生路径，确保业务可恢复，是当前业界探索的一个重要方向。

韧性网络与基础设施安全要求关注点不同,基础设施网络安全关注设备级业务安全攻击防护，韧性网络关注网络架构的高可靠和极端场景下业务的持续可用。目前韧性网络的定义和标准缺失，本文件提出了算力网络的韧性建网规范，指导建设故障可预警，冲击可防，业务可逃生的韧性网络，提升算力网络基础设施韧性，降低由于恶意、错误或故障造成损失的可能性和攻击导致业务中断或降级的程度，确保网络基础设施高可用。

算网融合 网络基础设施 IP 网络韧性规范

1 范围

本文件提出了算网融合网络基础设施韧性的基本定义、网络韧性等级分级标准、网络韧性评估总体框架和网络韧性能力评估标准，以及网络韧性在网元级、网络级、业务级和运维级不同层级的实施要点和建设标准。

本文件适用于监管部门、ICT服务提供商、服务集成商、设备提供商等组织开展算网融合网络基础设施韧性评估和规划实施工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

《NIST: NIST SP 800-160vol2》

《MITRE: Cyber Resiliency Engineering Framework 2009》

3 术语和定义

GB/T25069-2010界定的术语和定义以及下列术语和定义适用于本文件。

IP 网络韧性 IP network resilience

IP 网络韧性（IP Network Resilience）是指网络在遭受各种可能的故障、攻击或其他类型的扰动时，能够维持其功能、性能和服务质量的能力。

4 缩略语

下列缩略语适用于本文件。

ARP: 地址解析协议（Address Resolution Protocol）

BE:尽力而为(Best Effort)

BGP：边界网关协议 (Border gateway protocol)

BUM: 广播，未知单播，组播（Broadcast&Unknown-unicast&Multicast）

DDos：分布式拒绝服务 (distributed denial of service)

ERPS：以太环保护切换协议(Ethernet Ring Protection Switching)

IGP：内部网关协议 (Internal gateway protocol)

ISIS：中间系统到中间系统路由协议 (Intermediate System to Intermediate System)

LACP: 链路聚合控制协议（Link Aggregation Control Protocol）

LSDB：链路状态数据库 (Link State database)

MAC: 媒体访问控制地址（Media Access Control Address）

M-LAG: 跨设备链路聚合组（Multichassis Link Aggregation Group）

MTU: 最大传输单元(Maximum Transmission Unit)

NNI: 网络侧接口(Network-To-Network Interface)

OSPF：开放最短通路优先协议 (open shortest path first)

QoS: 服务质量(Quality of Service)

SID: 段标志符（Segment Identifier）

SRv6：基于 IPv6 的段路由(Segment Routing over IPv6)

STP：生成树协议 (Spanning Tree Protocol)

VPN：虚拟专用网络 (Virtual Private Network)

5 算网融合 IP 网络韧性概述

IP网络韧性（IP Network Resilience）是指网络在遭受各种可能的故障、攻击或其他类型的扰动时，能够维持其功能、性能和服务质量的能力。一个具有高韧性的网络可以在遭受攻击或故障时快速恢复正常运行，而不会对网络中的数据、用户或资源造成过大的损害。

IP网络韧性可以通过多种措施来提高，例如冗余备份、分布式架构、流量控制、安全认证等，以确保网络在面对各种挑战时能够保持高度的可靠性和可用性。

IP网络韧性一般可划分为五个阶段，分别是抵御阶段（Prevention）、检测阶段（Detection）、响应阶段（Response）、恢复阶段（Recovery）和适应阶段（Adaptation）。

a) 抵御阶段（Prevention）：在此阶段中，网络需要能够识别和防止威胁、攻击或故障的发生。网络需要部署安全措施，如防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等来保护网络和其上的应用和数据。

b) 检测阶段（Detection）：如果威胁或攻击发生了，网络需要能够及时检测到它们。在此阶段中，网络需要部署监控和检测系统，如安全信息和事件管理（SIEM）系统、网络流量分析工具等，来发现潜在的攻击或异常情况。

c) 响应阶段（Response）：一旦威胁或攻击被检测到，网络需要采取适当的措施来应对它们。在此阶段中，网络需要部署自动化响应系统、安全团队等，以进行快速反应和响应，最小化攻击或故障对网络的影响。

d) 恢复阶段（Recovery）：如果攻击或故障造成了网络中的某些部分受损，网络需要能够迅速恢复受损的部分，以确保网络的正常运行。在此阶段中，网络需要部署数据备份和恢复系统，以及快速恢复策略，以尽可能快地将网络恢复到正常状态。

e) 适应阶段（Adaptation）：最后，在不断变化的威胁和网络环境中，网络需要能够适应和调整自身的安全策略和架构。在此阶段中，网络需要进行持续的安全评估和改进，以确保网络的韧性和可靠性。

IP网络韧性的目标是提高网络的抗攻击能力和快速恢复能力，以保证网络的正常运行和业务连续性。IP网络韧性具有四个高级目标（Goal），分别是预期（Anticipate）、承受（Withstand）、适应（Adapt）、恢复（Recover）[来源：《NIST: NIST SP 800-160vol2》和《MITRE: Cyber Resiliency Engineering Framework 2009》]。

a) 预期目标：

指系统对不利情况是有准备的,潜在的威胁变成真正的不利事件时,系统有已定义的应对措施处理。在预期阶段，系统保持正常服务水平，韧性系统的预期目标包括系统对攻击、扰动和威胁的预防能力。

b) 承受目标：

指系统在被恶意入侵后还具备完成关键业务功能的能力,同时在一定程度上为系统的恢复和适应争取了缓冲的时间。在承受阶段，系统对攻击、扰动或威胁持续抵抗，韧性系统的承受目标包括网络在扰动下的自我调节和保障网络服务水平的能力，包括设备故障后的重新寻路、设备的保护机制等。

c) 适应目标：

指根据技术、操作或威胁环境中的预测变化修改任务、业务功能或支撑能力。在适应阶段，网络性能不再继续下降，韧性系统的适应目标包括网络对故障、扰动、攻击的快速识别、响应能力。

d) 恢复目标：

指系统在受到攻击的影响超出预期阶段的可承受范围之后可能出现关键任务和业务功能受损,这时应有一些预设的方案和技术确保在一定的时间窗内关键任务或业务功能恢复到正常进行。在恢复阶段，启动恢复措施，系统逐渐恢复到稳定的服务水平，韧性系统的恢复目标包括恢复措施的有效性以及服务水平的快速恢复能力。

6 算网融合 IP 网络韧性的分级和目标

6.1 IP 网络韧性分级

IP承载网的本质是持续的提供业务承载的能力,而IP网络韧性则是判断IP承载网持续提供业务能力的度量。通过对IP网络进行韧性评估，将网络进行量化和分级，有助于ICT服务提供商提前识别IP网络中的薄弱点，及时对网络进行调整，避免出现重大网络问题。

结合4.2中提到的4个高级目标，IP网络韧性的评估维度，可以根据下列细分因素综合分析确定：

a) 网络发生扰动后，网络业务受影响的程度：

通过冗余性和多样性的设计，可以保障网络在发生链路，节点或者站点故障时，网络可以快速感知故障并且倒换。不同等级的业务具有不同的保障设计，核心业务可以有热/温/冷备份和高QOS优先级的设计，确保任何情况下均可以自愈，非核心业务可以具备单次故障保护能力，但是在多次故障或者网络拥塞时业务会出现中断或者SLA质量下降。涉及的评估维度包括抗同时冲击次数、业务影响程度和业务恢复感知。

b） 网络发生扰动后，故障扩散范围：

一般情况下，网络出现故障后，网络中的业务在冗余性和多样性的设计下影响范围可控，但是在出现人为错误配置或者恶意攻击的情况下，网络故障会开始蔓延，极端情况下会扩散至整网，导致整网瘫痪。一个好的网络设计，应该将网络攻击或者故障限制在局部范围，确保整网的安全。

c） 网络发生扰动后，业务的恢复能力：

在网络出现攻击或者故障导致业务中断后，业务的恢复时间直接决定了网络最终的影响层度。由于网络管理本质上也是一种业务，如果在网络发生问题时，网管业务同其他业务一起中断，导致设备无法登录恢复业务，那么最终只能通过人工上站的方式恢复业务，业务影响时间将非常长。

d） 网络发生扰动后，网络的故障感知能力：

在网络出现攻击或者故障导致业务中断后，网络能够快速的感知故障，进行故障通告和溯源，帮助网络进行快速恢复，减少业务的影响时长。比如在算力网络中，可以建立一张网络数字地图，对于网络全景进行了动态绘制和动态刷新，实现网络拓扑清晰可视、网络路径透明追踪、故障传播关联溯源。

IP网络韧性等级可分为5级，如表1所示。

表 1　IP 网络韧性等级定义

韧性目标	韧性等级	L1	L2	L3	L4	L5
		铁级	铜级	银级	金级	钻石级
预期目标	抗同时冲击次数	0	1	2	3	4
承受目标	业务影响程度	＞30%	≤30%	≤20%	≤10%	≤5%
	业务恢复感知	天级	小时级	分钟级	秒级	毫秒级
适应目标	故障扩散范围	整网	整网	BGP 域	IGP 域	单站
恢复目标	网络恢复能力	弱	次弱	次强	强	强
	故障感知能力	弱	次弱	次强	强	强

6.2　IP 网络韧性目标

网络承受扰动分为以下3个抗扰动韧性目标：

a） Ⅰ类：承载核心流量的网络

例如IPCORE和算力承载网等，需要具备韧性综合等级L5级韧性等级，确保网络在发生各种意外情况下，核心业务可自愈，非核心业务影响范围小，可快速恢复业务；

b） Ⅱ类：普通承载网

承载传统的标准的话音业务的网络，要具备韧性综合等级L4级以上韧性等级，确保网络在发生各种意外情况下，核心业务可自愈，非核心业务影响范围小，可快速恢复业务；

c） Ⅲ类：internet 网

承载传统的标准的数据业务的网络，要具备韧性综合等级L3级以上韧性等级，确保网络在发生各种意外情况下，仍然能保持最低限度的业务保障能力；

以上为建议参考，具体情况可由运营商自行调整

7 算网融合 IP 网络韧性能力评估

7.1 IP 网络韧性评估目标

a） 评估 IP 网络韧性设计过程是否遵从韧性设计原则；

b） 评估 IP 网络韧性规格是否达到设计要求；

c） 评估现网韧性场景（失效/过载等）下客户关键业务可用性是否得到保持；

d） 评估网络遭受攻击/故障/扰动后，快速响应和恢复并保持服务水平的能力

7.2 IP 网络韧性评估要求

a） 可验证：评估项可以通过测试或者仿真验证；

b） 可度量：评估项有明确的评级标准；

c） 反馈改进：评估框架的演进，可以通过问题反馈，刷新评估标准、评估项和用例；

7.3 IP 网络韧性评估总体框架

IP网络韧性评估指标体系包括量化评测项和量化评分项，表1中6个评估维度与量化评测项、量化评分项对应关系如表2所示。

可直接通过业务进行IP网络韧性量化评测的部分称为“量化评测项”。对于暂时无法直接通过业务量化评测，但是跟IP网络韧性正相关的部分（比如网管可达快速恢复业务），可通过专家经验设置量化评分规则来评分，称为“量化评分项”。

表 2 IP 网络韧性评估总体框架

评估维度	量化评测项				量化评分项					
	业务通断	业务质量	影响用户	影响范围	版本补丁	操作容错性	故障隔离度	设备健壮性	网络可视度	管理可达性
抗同时冲击次数	●	●	●							
业务影响程度	●	●	●							
业务恢复感知	●	●	●							
故障扩散范围				●	●	●	●	●		
网络恢复能力										●
故障感知能力									●	

7.3.1 IP 网络韧性评估指标体系

IP网络韧性评估指标体系采用三级划分方式：第一级为维度，第二级为通用指标，第三级为专用指标，如图1所示。IP网络韧性指标体系计分方法如下：

a) 根据网络场景定义的专用指标上限、下限和计分方法，计算专用指标得分

b) 根据专用指标得分，汇总计算出对应通用指标的得分

c) 由通用指标得分加权汇总出维度得分，包括量化评测和量化评分

d) 由维度加权汇总出整个网络场景的 IP 网络韧性总分

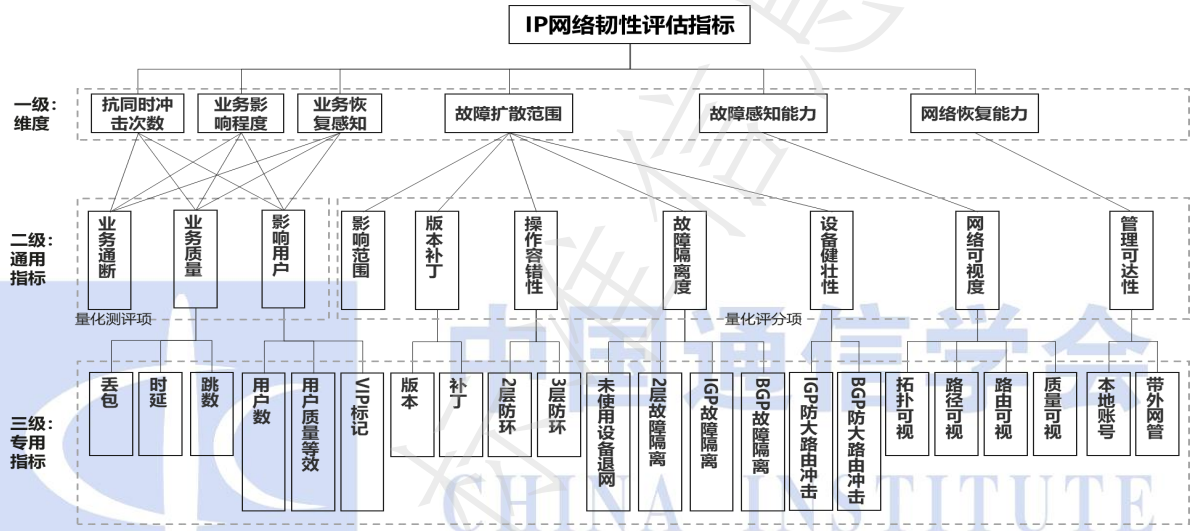

图 1 IP 网络韧性评估指标体系

7.3.1.1 量化评测项

量化评测项通过对网络注入扰动，通过评测扰动对于业务的影响来完成韧性的量化评估，如表3所示。

表 3 量化评测项

				业务通断	业务质量			影响用户			影响范围	
扰动类型	Flow	评测得分	Flow 类型	通|断	丢包	时延	跳数	用户数	用户质量等级	VIP 标记	影响标记	被影响标记
XX 扰动	Flow 1		S1	1								
XX 扰动	Flow 2		企业	0								
YY 扰动	Flow 1		S1	1								
YY 扰动	Flow 2		企业	0								

其中，量化评测项说明如下：

a) 业务通断，用于评估扰动发生时，业务流是否中断，通系数为1，断系数为0；

b) 业务质量，作为评估的权重，通过丢包，时延和跳数等对不同业务进行加权，丢包系数为0.5，不丢包系数为1，时延越限系数为0.8，不越限为1，跳数越限系数为0.8，不越限为1；

c) 影响用户，作为评估的权重，通过业务流的用户数，是否是VIP以及用户质量等级等对不同业务进行加权，用户数≥50为5分，≥10万为4分，≥3万为3分，≥1万为2分，≥1千为1分，企业用户为5分，用户质量等级为QoS等级（取值0到7），VIP标记为自定义（取值0到5）；

d) 影响范围，用于评估不同业务流之间的关联，比如信令流中断后，相关的业务流全部中断；

通过扰动库和故障遍历，算出每个扰动的韧性得分以及所有扰动的综合得分。

每一行得分为 = 业务通断系数×丢包系数×时延系数×跳数系数×(用户数+用户质量等级+VIP标记)×量化评分项总分。总得分 = 每一行得分总和

7.3.1.2 量化评分项

量化评分项是指针对无法通过扰动和业务直接完成韧性评估的指标，通过可量化的指标直接由网络专家完成评分，如表4所示。

表4 量化评分项

韧性目标	评分项	子项	分值	描述
预期阶段	版本补丁	在网设备版本和补丁符合要求	10	运营商提供网络最新软件和补丁，以此评估网络设备是否达标。根据满足要求的设备占比打分
承受/适应阶段	操作容错性	2层网络设备使能防环协议（STP或者ERPS等）	20	全部使能20分，2层网络中有一台未使能0分。如果有多个网络，则每个网络按照20分打分后取平均值。
		3层网络设备使能防环协议（OSPF，ISIS和BGP防环等）	20	有路由互引的设备如果都使能则20分，部分使能10分，全部没有使能则0分
	故障隔离度	未使用设备需退网	10	没有则为满分，有1例则0分
		2层故障域隔离（控制单2层广播域设备数量）	20	20分*（1减去一个2层域的设备占总设备的占比），多个域则取平均值
		IGP故障域隔离（减少路由协议互引）	20	没有互引20分，单向互引10分，双向互引5分。按照IGP域为纬度打分，有多个域则取平均值
		BGP故障域隔离（BGP路由策略对称，出方向的路由策略对端入方向也做相同控制）	20	双向控制20分，单向控制10分，没有控制0分
	设备健壮性	IGP防大路由冲击	15	满足要求的设备占比

		BGP 防大路由冲击	15	满足要求的设备占比
恢复阶段	网络故障感知	拓扑可视	5	网络有网管可以实时查看网络拓扑，有 5 分，没有 0 分
		路径可视	5	网络有网管可以实时查看网络业务路径，比如 srv6-policy 业务路径，srv6-be 业务路径，有则 5 分，没有则 0 分
		路由可视	5	IGP 和 BGP 实时监控&告警识别,有一个 2 分，二个都有 5 分
		质量可视（时延，带宽，丢包）	5	路由器使能如 TWAMP 或者 iFIT 等功能,网管可以实时看到网络质量，有则 5 分，没有则 0 分，如果部分网络使能则 2 分
	管理可达性	核心节点业务和网管分离(物理分离)	20	核心节点全部使能则 20 分，部分则 10 分，没有则 0 分
		接入节点业务和网管分离(物理分离或逻辑分离)	5	节点全部使能则 5 分，部分则 2 分，没有则 0 分
		定义本地登录账号	5	节点全部使能则 5 分，部分则 2 分，没有则 0 分

7.3.1.3 IP 网络韧性总分数

IP网络韧性评估得分如表5。每一级的分数和总分达标即可对应相应的定级。

表 5 IP 网络韧性评估得分

韧性等级	L1	L2	L3	L4	L5
	铁级	铜级	银级	金级	钻石级
抗同时冲击次数	0	1	2	3	4
业务影响程度	＞30%	≤30%	≤20%	≤10%	≤5%
业务恢复感知	天级	小时级	分钟级	秒级	毫秒级
得分（满分 200）	<140	≥140	≥160	≥180	≥190
故障扩散范围	整网	整网	BGP 域	IGP 域	单站
得分（满分 150）	≥0	≥0	≥45	≥90	≥140
网络恢复能力	弱	次弱	次强	强	强
得分（满分 20）	≥0	≥5	≥10	≥15	≥15
故障感知能力	弱	次弱	次强	强	强
得分（满分 30）	≥0	≥10	≥20	≥25	≥25
总分（满分 400）	<155	≥155	≥235	≥310	≥370

7.4 IP 网络韧性能力评估方法

7.4.1 评估方法总览

该评估应基于网络及业务的仿真并通过注入网络扰动的方式进行，以避免对现网环境造成损害，评估流程如下图所示：

1. 首先根据待评测网络的网络信息（拓扑结构、协议信息等）进行基础网络的还原，之后根据现网的业务部署情况，构建仿真业务流。由此得到待评测网络的网络及业务仿真模型。

2. 从预构建的扰动库中选取一条或者多条扰动注入上述网络业务仿真模型中。

3. 根据量化评测及量化评分细则进行各项打分（见6.3）

4. 网络韧性总分由各子项评分结果求和得出。

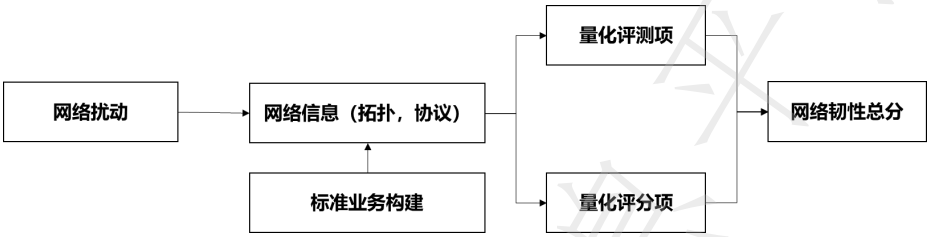

图 2　评估方法

7.4.2　扰动库构建

根据ENISA的定义，对正常操作的故障和挑战被称为对通信网络和服务的扰动。比如：

a)　无意的错误配置或操作错误：人为造成的非恶意错误；

b)　大规模的灾难（自然或者人为）；

c)　来自黑客的恶意攻击；

d)　硬件故障导致物理部件损坏；

e)　特殊事件导致的流量突增；

f)　其他运营商的网络故障引起的本地业务受损。

单次扰动对于整网业务的影响即为单次扰动IP网络韧性，所有扰动遍历对于整网业务的影响即为综合IP网络韧性。IP网络韧性的评估一般指综合的IP网络韧性。

初始扰动指的是网络中发生的一次原始的动作，比如光纤故障，一次错误配置变更等。次生扰动，指的是初始扰动发生后，网络中的状态变化，进而最终对业务的影响。

通过构建网络扰动库，对网络进行评估来量化IP网络韧性，扰动库构建如表6所示。

在网络扰动库构建完成后，需要通过扰动对网络进行评估。有2种模式参考：

a)　通过 Netflix 公司提出的混沌工程的方式，在整个网络中在随机位置主动制造扰动，测试网络在各种扰动下的行为，识别并修复故障问题，以此快速了解网络是否健壮，是否可以处理计划外的故障。混沌工程的方式会对现网造成业务影响，需要严格测试的时间和范围。

b)　通过网络仿真的方式，将现网镜像到仿真系统，在仿真系统中遍历所有扰动，以此来对网络做韧性评估。推荐使用仿真的方式来做评估，对网络影响最小。

表 6　扰动库构建

序号	评估场景	子场景	次生扰动	初始扰动	评估点

1	生存性评估	故障遍历扰动	不限定	1、全网节点&NNI 链路单点故障遍历 2、全网节点&NNI 链路双点故障遍历	通过单&双链路故障，识别网络中断业务流，绕行业务流，拥塞业务流（以及拥塞链路）。发现网络可靠性设计薄弱点。
		核心资产扰动	DNS 路由，Radius 路由，网络管理路由等核心路由消失	1、识别核心资产位置，通过 UNI 链路故障或者节点故障或者引入错误路由策略的方式遍历	通过攻击核心资产，识别网络影响范围
2	环路评估	3 层环路扰动	3 层路由环路	1、OSPF 进程互引 2、ISIS 进程互引 3、OSPF 引入 ISIS 4、ISIS 引入 OSPF 5、OSPF 引入 BGP 6、BGP 引入 OSPF 7、ISIS 引入 BGP 8、BGP 引入 ISIS	通过 3 层环路评估多少业务受损，以及环路扩散的范围。
		2 层环路扰动	2 层路由环路	1、新增链路 2、修改 VLAN 方式	通过 2 层环路评估多少业务受损，以及环路扩散的范围。
3	大路由冲击评估	BGP 大路由冲击评估	BGP 发布大量路由给邻居	BGP 关键节点通过路由策略引入大量路由给邻居（模拟加拿大 Rogers 事故）	1、如果没有设备规格信息，则评估路由扩散范围，哪些网元受到影响； 2、如果有设备规格信息，可以直接评估出受损网元； （注：可以建立规格库的方式做一定的评估，无法支持的只能评估影响范围）
		IGP/MPLS 大路由冲击评估	IGP 中泛洪大量路由	BGP 关键节点通过路由策略引入大量路由到 IGP	1、如果没有设备规格信息，则评估路由扩散范围，哪些网元受到影响； 2、如果有设备规格信息，可以直接评估出受损网元； （注：可以建立规格库的方式做一定的评估，无法支持的只能评估影响范围）
4	恶意安全攻击评估	DDos 攻击	网络中出现大量流量攻击	在网络中注入大量攻击流量	评估网络是否有 DDos 的防御能力，评估业务影响范围
		恶意登录	网络中出现非法地址登录设备	在网络中用非法地址尝试登录设备	评估设备是否有访问控制，限定非法登录

7.4.3 业务流构建

网络信息的构建是IP网络韧性评估的另一个前提，网络信息构建需要包括网络拓扑和网络协议。业务流用于评估扰动对于网络业务的影响，同时也作为不同IP网络韧性评分的基准，如表7所示。

表 7 业务流构建

Flow 名	Flow 类型	源节点名	宿节点名	源 IP	宿 IP	流量大小(Mbit/s)	用户数	用户质量等级	是否为 VIP 业务
Flow1	单播	S1	D1	192.168.1.1	172.16.1.1	100	10 万	5	否

其中，业务流字段定义如下：

a) Flow 名：自定义名字，用于区分不同流

b) Flow 类型：单播，组播

c) 源节点名：始发设备名字

d) 宿节点名：目的设备名字

e) 源 IP：业务源 IP 地址

f) 宿 IP：业务目的 IP 地址

g) 流量大小：该条业务承载的流量大小，单位 Mbit/s

h) 用户数：该条业务承载的用户数量

i) 用户质量等级：一般与业务流的 QOS 优先级相同

j) 是否为 VIP 业务：该业务是否承载 VIP 用户

8 算网融合 IP 网络韧性能力要求

8.1 总体要求

IP网络韧性能力增强要求包括4个纬度，网元级、网络级、业务级和运维级。

8.2 网元韧性能力要求

网元韧性能力要求网元韧性需满足如下要求：

a) IGP 具备防止大路由冲击的能力，在引入或者学习到大量路由导致内存过载时，设备要有保护机制，确保内存不会继续劣化，不会导致网络中其他设备内存过载

b) BGP 具备防止大路由冲击的能力，在学习到大量路由导致内存过载时，设备要有保护机制，内存超限后不接收新路由，不中断邻居

c) 设备 IGP 和 BGP 支持路由互引环路检测

d) SRv6 Policy 算路场景，设备需要支持并且开启 BGP Policy GR 能力，在 SRv6 Policy Server 故障场景下，可以保持 SRv6 Policy 路由，并支持极端情况下的 SRv6 BE 逃生能力，避免业务中断

e) 部署 SRv6 Policy 的网络设备需要支持报文压缩能力，在网络中存在微波或者租用链路，并且短期内无法扩容时，可以部署缓解网络拥塞

f) IPv6 路由器支持 SEND 协议来防止 NDP 报文仿冒威胁和 DDOS 攻击

8.3 网络级韧性能力要求

8.3.1 冗余多样规划

网络设计应当保持冗余和多样性。冗余规划应当从物理层和协议层考虑。

在物理层设计中，链路和节点要有冗余备份设计，在冗余设计基础需要关注共光纤/共SRLG/共单板风险，做到多样性设计，避免出现假冗余，单点故障，应：

a) 建议网状连接或者半网状连接，尽量避免流量跨越多个核心节点。考虑到流量多数为到核心层流量，建议汇聚层设备采用双归属到核心层设备；
b) 如果拓扑结构涉及到双上行，如果条件允许，上行口需要分布在不同的业务板上
c) 网络中关键节点保证双设备、双链路
d) 网络关键设备主控板、交换网板、电源、风扇实现冗余备份
e) 网络中关键节点保证存在异地容灾保护
f) 在协议层设计中，需要考虑主备路径的设计，且应尽量避免主备路径间有任何的重叠部分。

8.3.2 故障隔离规划

网络设计分层分域是避免大规模网络事故的关键设计，应：

a) 在 IP 网络设计中，若二层和三层方案均能满足客户业务需求且设备无特殊限制的前提下，建议优先考虑三层方案。如果无法实现，那么对于纯 2 层组网，应当控制 2 层广播域的规模，同时针对 2 层广播域的接口要配置合理的 BUM 控制
b) 对于单 LSDB IGP 域，应当控制一个进程的设备数量，减少网络震荡带来的协议风险
c) 对于物理规模域，应当控制接入环，汇聚环和核心网所带设备数量
d) 对于网管管理域，应当控制单网管管理设备数量
e) 对于时钟信号，需要从接入侧，汇聚侧做好隔离控制，避免出现环路或者优选下级时钟
f) 业务接入节点和接口对于网络业务要 0 信任，需要对接口做 QoS 优先级，限速等控制

8.4 业务级 IP 网络韧性能力要求

有限资源应该用于防护关键核心资产，即在有限的资源下对关键资产进行防护。首先需要定义关键资产，比如核心节点，核心链路，DNS路由，Radius Server等，然后对关键资产进行网络设计与监控保护。网络可视对于问题快速感知、定位和恢复有非常大的帮助。针对关键资产进行监控，当关键资产发生变化时，快速感知和恢复：

a) 网络拓扑可视
b) 网络路径可视
c) 路由可视，针对关键节点路由进行监控
d) 网络质量可视（丢包，时延，带宽），网络出现问题可快速感知，快速定位
e) 信息自动更新
f) 对关键资产进行监控，出现异常可快速定位

如果网络设计不合理，业务侧的一些异常往往会造成网络发生重大故障，针对业务侧的韧性，需要考虑：

a) 合理的 QoS 设计，针对边缘侧业务接口，对于信任的业务，需要配置合理的 DSCP 映射，对于不信任的业务，需要配置严格的限速和非信任的 DSCP 映射，防止业务出现错误的高优先级大流量影响网络侧业务；

b) 对于 2 层边缘接口，需要配置 BUM 限制等，防止业务成环影响网络侧业务；

c) 对于用户侧对接 BGP 场景，需要策略严格控制路由收发，防止用户侧错误路由影响网络侧业务；

8.5 运维级韧性能力要求

8.5.1 网络管理规划

网络设备管理是网络事故的最后一道防线，只要设备不宕机，就要确保能登录。可考虑的方案有：

a) 带外网管，确保业务和管理完全隔离，在业务受到重大冲击时，可登录设备

b) 需要定义本地认证账号，在外部认证不可达时，可登录设备

c) 网络管理关键资产要多样化，比如站点门禁和设备远程管理不应该被一套系统定义，否则出现问题时现场和远程都无法启动业务恢复

d) 对于网络管理的路由和 QoS 需要做高优先级设计，确保在出现极端情况下，网络管理路由可达，设备可登录

8.5.2 故障恢复规划

a) 针对关键资产要定义应急预案

b) 维护人员需要有 2 个以上运营商 SIM 卡

c) 核心路由监控方案，核心路由出现异常，上报告警

d) 全网配置备份和监控方案，配置发生变化时可感知，可快速恢复

8.5.3 操作容错规划

网络操作的容错规划可从用户操作的三个阶段来考虑，即操作前、操作中、操作后。可大致归纳为以下几方面内容：首先在用户操作前提前识别清理网络风险；其次在重要的操作步骤给予用户及时有效的提示；当用户发生操作错误或失误时及时为用户纠错并提供有效的解决方案；最后帮助用户在错误发生后迅速回到正确状态。

a) 网络设计增加操作容错性

- 比如交换机的设计，考虑M-LAG优于堆叠的设计
- 网络侧NNI接口推荐使用LACP的链路捆绑
- 关键节点设置路由接收limit
- 减少协议路由互引的设计，杜绝互引引发路由环路
- 路由接收纯2层组网，是否开启防环协议（STP，ERPS）

- 未使用设备及时退网

b) 操作前

- 提前Audit识别网络冲突的IP，路由和MTU等
- 提前Audit识别网络关键配置是否错误或者遗漏，尤其是防环类
- 提前Audit识别网络是否有环路
- 提前Audit识别业务系统和网络设备是否已经存在告警，需要清理确保没有潜在风险后启动操作
- 提前分析识别割接相关业务流，确保割接后业务可验证
- 提前备份网络配置，采集路由，MAC，ARP，流量等表项，确保割接后可对比验证
- 操作前的方案仿真验证，识别网络变化是否符合预期

c) 操作中

- 高危操作有确认
- 错误操作可拦截
- 资源超限可避免
- 资源超限不中断
- 操作有规范，推荐使用工具下发，避免人为低级错误
- 操作过程中需要时刻监控核心资产的路由和流量，业务系统的告警，出现操作预测外的异常需要及时处理
- 操作完成后可针对有备份路径的业务做一次倒换验证，确保备份路径可生效

d) 操作后

- 启动babysitting，对网络核心资产的运营状态进行监控，出现异常后快速预警与恢复
- 清理业务系统和网络设备告警，操作外的未知告警需要定位确保网络无异常
- 及时备份操作后的网络配置
- 及时更新网络inventory系统
- 检查网络中是否有操作遗留的垃圾配置，操作范围内的需及时清理