国 际 电 信 联 盟

ITU-T Y.1271

国际电信联盟
电信标准化部门

(07/2014)

Y系列：全球信息基础设施，
互联网的协议问题和下一代网络

互联网的协议问题 – 体系、接入、网络能力和资源管理

演进中的电路交换和分组交换网络支持应急通信的网络要求和能力的基本框架

ITU-T Y.1271 建议书

国际电信联盟

ITU-T Y 系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	**Y.1200–Y.1299**
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
通过下一代网络提供IPTV	Y.1900–Y.1999
下一代网络	
框架和功能架构模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
基于分组的网络	Y.2600–Y.2699
安全	Y.2700–Y.2799
通用移动性	Y.2800–Y.2899
运营商级开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500–Y.3999

欲进一步了解详细信息，请查阅ITU-T建议书清单。

ITU-T Y.1271 建议书

演进中的电路交换和分组交换网络支持应急通信的网络要求和能力的基本框架

摘要

在不断演进的电路交换和分组交换电信网络中，要定义并确立支持应急通信的能力，会面临很多的挑战并需要深思熟虑。本建议书对演进中的网络有能力提供的应急通信的基本需求、特性以及概念等进行概述。

历史沿革

版本	建议书	批准日期	研究组	唯一的ID*
1.0	ITU-T Y.1271	2004-10-14	13	11.1002/1000/7047
2.0	ITU-T Y.1271	2014-07-18	13	11.1002/1000/12177

* 要获取该建议书，请在您网页浏览器的地址栏中输入以下URL：“http://handle.itu.int/”以及建议书的唯一ID号。例如：http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2014

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

引言

应急通信目的是为应急恢复工作提供帮助以重建社会基础设施，使人们能够在严重的灾害之后恢复正常的生活状态。在一些国家，应急恢复工作属于公共安全机构的责任。响应者需要评估灾害损伤程度，协调救援、医疗救助和重建工作等。为实现这一目的，可以通过共享公共电信基础设施的资源来实现应急通信，在一些情况下，可以使用企业网的附加资源（如公共安全网）。这些公共电信基础设施正在由基本电路交换向具有不同的通信能力的分组交换网络演进。

ITU-T Y.1271 建议书

演进中的电路交换和分组交换网络支持
应急通信的网络要求和能力框架

1 范围

要定位应急通信所面临的前所未有的挑战，就需要了解其来龙去脉并仔细思考。本建议书对演进中的网络有能力提供的应急通信的基本需求、特性以及概念等进行概述。本建议书在支持应急通信的网络要具备的要求和能力方面为电信网络运营商提供指导，并在如何请求（获取）这些能力方面为响应者（用户）提供有用信息。

注 – 本建议书定义了一些要求，满足这些要求的网络将有助于支持应急通信服务，并且在必要时可以推动[ITU-T E.106]和[ITU-T E.107]建议书的应用。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书或其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

[ITU-T E.106] Recommendation ITU-T E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

[ITU-T E.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[ITU-T J.260] Recommendation ITU-T J.260 (2005), *Requirements for preferential telecommunications over IPCablecom networks*.

[ITU-T J.261] Recommendation ITU-T J.261 (2009), *Framework for implementing preferential telecommunications in IPCablecom and IPCablecom2 networks*.

[ITU-T M.3342] Recommendation ITU-T M.3342 (2006), *Guidelines for the definition of SLA representation templates*.

[ITU-T X.1303] Recommendation ITU-T X.1303 (2007), *Common alerting protocol (CAP 1.1)*.

[ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[ITU-T Y.2205] Recommendation ITU-T Y.2205 (2011), *Next Generation Networks – Emergency telecommunications – Technical considerations*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2013), *Cloud computing infrastructure requirements*.

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2013), *Cloud computing framework for end to end resource management*.

[ATIS-1000057] ATIS-1000057 (2014), *Service Requirements for Emergency Telecommunications Service (ETS) in Next Generation Network (NGN).*

[ETSI TS 122 011] ETSI TS 122 011 (2013), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Service accessibility (3GPP TS 22.011 version 11.3.0 Release 11).*

[ETSI TS 133 401] ETSI TS 133 401 (2013), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 11.7.0 Release 11).*

[IETF RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP).*

[IETF RFC 5321] IETF RFC 5321 (2008), *Simple Mail Transfer Protocol*.

[IETF RFC 5670] IETF RFC 5670 (2009), *Metering and Marking Behaviour of PCN-Nodes*.

[IETF RFC 6679] IETF RFC 6679 (2012), *Explicit Congestion Notification (ECN) for RTP over UDP*.

[IETF RFC 6710] IETF RFC 6710 (2012), *Simple Mail Transfer Protocol Extension for Message Transfer Priorities*.

3 定义

3.1 其他地方定义的术语

本建议书使用了以下其他地方定义的术语：

3.1.1 应急通信服务（ETS）[ITU-T E.107]：国家服务，它在发生灾害和出现突发事件时向有权使用ETS的用户提供优先通信。

3.1.2 下一代网络（NGN）[ITU-T Y.2001]：下一代网络是一个能够提供电信业务并能使用多种宽带、可实现服务质量（QoS）的传输技术的分组网络。在此网络中，有关服务的功能独立于底层传输技术。它使用户不受约束地接入网络及竞争服务提供商和/或其所选择的服务。它支持一般性移动，由此可为用户提供连贯一致的及无处不在的服务。

3.2 本建议书定义的术语

本建议书规定下列术语：

3.2.1 保障能力：能够为关键通信的可用性和可靠实施提供高信任度或完全保证的能力。

3.2.2 认证：核实一个声称的身份的行为或方法。

3.2.3 授权：决定是否给予特别凭证的提交者某些特别权利（比如访问电信资源）的行为。

3.2.4 授权的应急通信用户：经过授权，在国家和/或国际紧急情况下可以获得额外特权和能力的个人或组织。

3.2.5 自下而上的紧急上报：由个体用户对认为或确定的紧急情况进行上报。用户可以根据各自的授权和权力使用应急通信能力。

3.2.6 缓冲膨胀：当分组交换网中不同网络节点和终端系统的大过滤器造成额外延迟和抖动并削弱整体网络性能时的情况。这种情况可能影响应急情况的传递速度。

3.2.7 有限的紧急情况：在一个地理范围相关小的区域（比如局部）内发生的紧急情况，不影响其他地区。

3.2.8 上报的紧急情况：由相应政府中权威的职能部门公开认可和声明的紧急情况。

3.2.9 紧急情况：突然和出乎意料发生的并且性质严重的情况。这时需要借助电信手段，采取广泛、迅速和重大的措施使得情况恢复到正常状态，避免生命和财产损失的风险。如果这种情况持续发展，可能演变成为危机和/或灾难。

3.2.10 国际紧急情况：超越边境，影响多个国家的紧急情况。

3.2.11 标签：附着或包含在数据单元中的标识符。

3.2.12 全国性紧急情况：影响整个国家，但是仅限于一个国家内的紧急情况。

3.2.13 常规应急能力：电信能力中一种特殊的应急种类（比如911，110或112），在国家的层面上用于让公众向政府部门或其他官方授权的民间机构汇报本地或个人的紧急情况。

3.2.14 政策：根据不同的标签，为不同种类的通信业务分配电信网络资源的规则（或方法）。

3.2.15 优先权：具有特权能够或易于获得相对于他人的优先。

3.2.16 优待权：能够获得比一般性能力更强的能力。

3.2.17 拥塞控制中的优先处理机制：为缩小拥塞对应急通信的影响而对电信资源进行管理的方法。可通过诸如网络设计、网元机制（如机器拥塞控制）和网络操作能力等多项措施管理拥塞问题。

3.2.18 优先权处理能力：提供特别的接入和/或使用电信网络资源的能力。

3.2.19 公共安全：一些区域使用该概括性词汇以涵盖为大众福祉和保护公众配合其它诸如消防和救援、救护和紧急医疗服务、警察和安全保卫许可等多项服务的应急恢复工作。预防和防止大众遇到影响安全的犯罪或灾害等险情为主要目标。

3.2.20 自上而下的紧急发布：经过授权的政府或行业的职能部门发布的紧急情况通告。

4 缩略语和首字母缩写

本建议书采用下列缩略语和首字母缩写：

CSP 云服务提供商

DSL 数字用户线路

ETS 应急通信服务

GBR 保障速率

IM 即时消息

IMS IP多媒体子系统

KQI 关键质量指标

LTE 长期演进

NGN 下一代网络

QoS 服务质量

RACH 随机接入信道

RAN 无线接入网

SLA 服务等级协议

SLS 服务等级规范

SMS 短信服务

SMTP 简单邮件传送协议

SP 服务提供商

5 安全

根据本建议书的性质，安全问题会被一般性的提及。然而，对于第6.3和第7节一些与安全有很相关性的要求，应该引起特别的注意，比如授权（第6.3节）、网络完整性（第7.2节），特定用户的保密（第7.3节），网络可恢复性（第7.4节），互操作能力（第7.6节），生存能力/抗毁性（第7.9节）和可靠性/可用性（第7.15节）。ITU-T的其他建议书可能会对本建议书的安全方面进行补充和完善。

6 探讨

6.1 紧急情况的性质

灾难通常以突发事件的形式发生并造成巨大破坏、损失和毁灭。灾难的发生可能源于大自然的威力，也可能源于人类对自然的干涉或者由人类自身行为滋生。灾难可以强度很大，持续时间很久，并覆盖很广的地理范围，可以是全国性的也可以是国际性的。总之，各种灾难在强度、持续时间及影响范围上存在不同。

全世界每年发生数以百计的灾难，没有国家可以幸免。在限定范围内发生的灾难虽然可能非常严重，但在性质上仍然被定义为局部灾难。灾难也可能影响整个地区，甚至造成全国或国际性的紧急情况。每一个灾难都会对经济及社会秩序造成影响。无论何种灾难，都要求电信系统做出有效反应以协助挽救生命。

为预测和有效应对灾害，多数国家已设计并部署了规划和措施（如测试、演习和练习）。然而，有时可能会出现所谓“黑天鹅”情况。异常状况的非正常组合可能会对传统的灾害预测和减灾方式造成挑战或威胁。

6.2 应急响应

由自然或人类自身引起的各种灾难，可能在任何时间、任何地点向我们发起攻击。灾难的恢复需要分阶段进行。灾难的第一响应对于受灾程度评估和控制损失非常重要，而其他阶段措施要快速跟进。在第二阶段优先考虑的事情是处理伤员和挽救生命。第三阶段通常是从其他地区及资源储备点调集后备救灾人员、物质和装备。第四阶段是清理和重建。

对于灾难恢复的整个过程而言，贯穿其中的就是要求应急通信能够被快速、稳定和易于掌握地使用，可以依靠技术手段和/或政策手段来实现这种要求。应指出，现有最初为各种逆境设计的规划可能要比这些响应措施的级别更低，举例而言，地震的强度可能超过规划内措施的应对水平。

6.3 通信保障

通信保障目的是在紧急情况下确保通信的能力。灾难本身会对电信基础设施造成冲击。典型的影响还包括：拥塞、过载，以及需要将通信能力重新分配或扩展到现有网络没有覆盖的新地理区域。就算基础设施没有被灾难破坏，在发生这些事件时对通讯的需求也会急剧增长。

紧急情况发生时，可以通过各种方式通知职能部门。可以由居民运用一般的应急手段通知职能部门灾难的到来，也可以由那些直接或间接与受灾民众接触的应急人员自下而上的进行紧急情况上报。这些信息可能最终导致相关的政府职能部门宣布紧急情况，然后是自上而下的紧急情况发布。

在真正的紧急情况到来前，应该事先掌握应急人员的联系方式。这些人员的通信凭证应该被保存下来，以便于他们能够通过需要授权的电信网络的认证。通常，在提供优待和优先通信能力（如优先于其他用户）时，服务使用者需获得授权和认证。 是否需要授权依照各个国家内部的规定。但是如果没有授权制度，可能会导致优先权被非授权的个体滥用。有关安全的技术设详见ITU-T Y.2205建议书的第11节。

电路交换和一些分组交换网络（下一代网络[NGN]）应对过载的方法就是当系统饱和后拒绝所有的呼叫。一些网络向所有请求提供优待处理。一种选择是当经过授权的应急通信人员需要进行通信时，占先于其他呼叫者。然而，某些种类网络在增加额外的载荷时，会降低整个网络的性能。这种情况通常发生在以“尽力而为”为框架模式的网络当中，在这里所有的信息都被平等对待，在没有资源可用时信息只是简单的排队等待或者最终被丢弃。

最近的研究和测量表明，所谓“缓冲膨胀”的现象可能导致无法容忍的延迟。内存成本的下降促使（包括宽带网中最终用户设备在内）网络资源拥有强大的缓冲器。这些缓冲器造成旨在降低拥塞影响的拥塞通知的延迟。这些大缓冲器不仅会影响到尽力而为的业务，还会影响到包括应急通信在内的优先业务。

为应急通信提供优先权，并建立具有一点容错性、不会因某一个部件损坏而造成整体瘫痪的网络，是迈向通信能力保障的重要步骤。虽然网络的容错性对通信能力保障非常关键，但是网络运营者仍然应该制定恢复预案，以便于在网络瘫痪时尽快修复网络。

7 应急通信的要求和能力

完全意义上的应急通信需要具备多种能力，以支撑紧急救援人员的各种通信需求。在表1中列出了一些特定的目标和要求，这些要求有利于救灾行动中的通信。如果能够在网络的运营中贯彻这些要求，将在紧急事件发生时极大的促进救灾工作的效率和及时性。

注 – 如果某个解决方案可以满足如下这些要求，那么它也可以被应用于传统的应急服务中，如110，112，或911等。对满足这些要求和条件的请求应是各国的内部问题。

表1描述了这些目标及功能要求。

表1 – 应急通信功能要求和能力

增强的优先权处理
安全的网络
位置保密
可恢复性
网络连通性
互操作性
移动性
普遍覆盖
生存能力/抗毁性
语音传输
视频传输
数据传输
可变的带宽
可靠性/可用性
拥塞控制机制中的优待处理

7.1 增强的优先权处理

应急通信话务流在穿越任何网络时都需要获得保障。保障能力的一个重要组成部分就是增强的优先权处理。实现优先权处理的一种可能方法是，首先“标记”应急通信业务（比如分类和/或使用标签），并对这种话务流应用网络策略，以达到所需的服务保障。在面向连接的传输中，一旦连接被建立，呼叫实际上是“固定连接”的，不需要进一步的标记优先状态也能够保证质量。然而对于无连接的分组交换传输，必须为每一个数据包添加应急通信标识。电信网络运营者和业务提供者（SP）需要根据他们和用户签署的SLA，识别并优先处理应急通信。

网络运营者需要为新的或临时的应急作业用户预备接入线[1]，并且接入线应该基于优先的基础，以保证应急通信能够被快速的开展。

7.1.1 优先接入电信设施

访问电信资源并获得应急通信能力的途径有很多，包括模拟用户线、无线、卫星、有线电视电缆、数字用户线（DSL）以及光纤。如果在各种通信网络上都能够获得优先的接入服务，对于应急作业用户来说是非常有利的，这样能够更快速的开展应急通信。

传统的电路交换网络通常没有为优先接入需求在信令上做准备。可以通过特殊标记的用户线或特殊的“摘机”业务来提供优先接入，但是这仅仅是针对特定位置的特定用户线，不能满足所有应急通信的需求。目前在使用传统的电话设备进行接入时，在拨号音或业务发起信息内无法携带优先权。拨号音的产生受限于端口数量，并且在重载的情况下对端口的消耗会造成接入的延迟。因此对于演进中的网络，应该考虑具备支持业务优先接入的能力。

7.1.2 优先建立、使用剩余的可控资源并完成应急通信

为了将应急通信业务和一般通信业务区别开来，需要对其进行识别。在传统的电路交换网络上，只有通过信令协议才能区分两种通信业务。而在分组交换网络中，可以通过在信令和数据单元上使用标签来实现不同种类通信业务的区分。在分组交换网络中，标签可以被放置在不同的协议层或子层中。

通信业务被识别后，电信网络的策略或方法将被应用于对应急通信业务的增强优先权处理。对于面向连接的传输，这种策略意味着呼叫请求被接受的概率更高；对于无连接的传输，这种策略意味比一般的通信业务具有更高的路由和传送成功率。

7.1.2.1 拥塞中紧急业务的接通

在网络拥塞中，需将对紧急业务的影响降至最低水平。传统的电路交换网使用诸如呼叫拦截等业务控制方法以减轻网络拥塞。应急业务的区别在于尽量减少拦截并确保高水平的普通业务呼叫接通率。

在分组交换NGN中，针对应急业务的优先信令、信令和媒体的优先传送以及各种优先处理机制（包括拥塞控制机制）用来防止拦截并确保紧急业务具有高于普通业务的接通率。

7.1.2.2 免于网管控制

根据区域/国家要求和网络运营商的政策，应急通信应免受网管控制，除非进一步豁免将造成网络的不稳定性。拥塞控制（如机器拥塞控制）、超载控制和负载平衡不得对应急通信造成不良影响。

---

1 在文中提及的接入线，既包括有线接入，也包括无线接入、信道、虚连接以及隧道等。

7.1.3 应急通信业务的优先路由

某些情况下，当默认路径已经不可用或拥塞时，应急通信业务应该被重定向到备用路径上。在演进的网络中，要求应急通信避免单点故障，因此当在分组交换网络中出现过载或连接失败时，应该有多条备用路径或可选路由可以被启用。对于一次呼叫来说，对数据包的路由是一个持续的过程，直到这个会话结束。因此，业务监测和网络控制应持续不断，以避免超载连接和系统造成的影响。此外，大缓冲器超载的影响可跨越不同网元，造成可用实际带宽的差异。因此，不断监测和控制可用来管理缓冲器并避免应急业务的大量延迟。

此外，可部署近年来面世的一些新的防止拥塞技术（不同于拥塞控制）以便为应急通信用户提供支持[IETF RFC 4412] [b-IETF RFC 5559] [IETF RFC 5670]和[IETF RFC 6679]。

7.1.4 可选的对非应急通信业务的占先

占先的概念通常被用于基于电路交换的通信，在一些分组交换（NGN）网中的应用亦有定义。对非应急通信业务的占先指的是非应急通信业务为应急通信释放带宽和资源，这是一个可选要求。基本的应急通信措施中不包括占先的概念。

7.1.5 在基础资源不可用时，允许降低通信业务的服务质量

应急通信业务的QoS一般来讲会被设为最高，以确保干净清晰的通信及重要信息的携带。然而，在电信资源承受沉重压力时，对QoS进行适当的降级也是可以接受的。这种情况仅仅发生在资源损失非常严重，已经到了网络即无法支持非应急通信业务，也没有足够的带宽和资源来保证应急通信业务正常的QoS水平的地步。对于应急作业人员来说，即使不能达到完全满意的程度，只要还能持续的传递关键的信息，就比失去通信能力要强。

在紧急情况下并且电信基础资源即将耗尽时，需要给予应急通信比一般通信更高的优先权。这可能会影响已经建立的通信的QoS，因此，一个正在进行中的通信可能被降级甚至被释放。

7.2 安全的网络

安全保护是必须的，以防止未授权用户使用支持应急作业人员所需的稀缺电信资源。

7.2.1 在应急通信中对认证用户的快速授权

应急通信仅提供给参与应急恢复作业，且通过授权的用户使用。每个国家或共同体的相关机构会对它们的指定用户进行核准。对于演进的网络（包括移动网络），从发起应急通信请求开始，就需要有一种创新的方法来实现用户的快速授权处理，验证用户身份，保护电信资源在紧急情况下不被滥用。一旦授权通过，应急通信业务开始穿越网络，授权信息就需要映射到标签上，并从呼叫的发起到呼叫的终结一直传送。在整个应急呼叫的过程中标签都必须被保留。

7.2.2 应急通信业务的安全保护

除了认证和授权外，其他方面的安全需求，比如防欺骗、防非法入侵和防拒绝服务攻击等，在应急通信中同样需要。除此以外，还要提供一种额外保障来发现没有获得授权的修改。网络增强了防止非法入侵和防止拒绝服务攻击的能力，一般的通信也能因为而获益。网络应该在话务流和控制流中，适当的使用扩展的加密技术和用户授权，以防止欺骗和未授权的接入。

7.3 位置保密

对于某些应急通信，需要应用特别的安全手段。比如，当阻止灾难救援人员的行动也成为了破坏行为的一部分时。这种情况下，由特定用户发出的应急通信因为性质紧急并且重要，应该保证不被他人操纵、监听或阻碍。这时需要运用特别的安全机制，来防止将应急通信用户的位置信息暴露给未授权用户，以保护认证用户不被定位。这些特别的安全要求超越了本建议书的框架范围。

少数处于高级领导层的应急通信用户在组织应急减灾行动时，决不能面临位置被发现的风险。

7.4 可恢复性

如果网络中实施应急作业的一些关键能力瘫痪，这些能力需要被尽快恢复。无论电路交换还是分组交换网络，都需要通过物理接入线（有线的或无线的）将网络延伸到用户所在位置。如果接入线毁损，网络运营者即使恢复运营，接入也要中断很长时间。因此，网络有必要具有优先恢复的能力，以使得应急通信能够尽快开展。

中断发生时，电信网络应该有能力被完全修复，或至少被恢复到能支持优先通信的水平。

7.5 网络连通性

支持应急通信的网络需要和其他网络连接起来，以扩大网络触及的范围。在连接各国应急通信网络的国际边界节点上实现优先权处理的互通，就可以建成国际应急系统，比如，可以应用[ITU-T E.106]和/或[ITU-T E.107]建议书。

注 — 灾难通常是区域性的，但是这个区域内可能包括多个国家。此时多个国家的灾难恢复应急通信可能需要对同一个特殊事件进行响应。并且，在“日益网络化的世界”里，很多国家会为受灾国家提供灾害救助支持。

在自由竞争的环境下，可能出现如下情况：

a) 一个国家内有多个网络运营者；

b) 一个网络运营者的网络延伸到多个国家。

这时，需要对网络运营者之间及跨越国家边境的网络的应急通信互通能力给予考虑。

7.6 互操作性

对于演进的网络来说，面临很多问题。其中一个就是如何能够有序和透明的确保[ITU-T E.106]建议书中的基本应急优先选择能力。在融合时期，需要从多方面考虑电路交换技术和分组交换技术的互通问题。比如，从固定或移动网络产生的语音呼叫，可能先经过分组交换网络，然后又终结到电路交换网中，或者直接终结在分组交换网络中。ITU-T J.261第6节和ITU-T J.261第6.2节负责处理PSTN和IPCablecom网络的优先处理方法。这些要求可能适用于其它异构网络。

构造问题通常是协同工作中的一个主要问题。为了在提供应急通信的不同的运营者之间实现互操作，应该采用通用的构造。但是需要注意的是，这并不是说网络运营者如果想要支持应急通信，就必须在他们网络的内全部使用相同的构造，他们只需要在网络的出/入口位置对构造进行适当的转换就可以了。这种方法具有普遍性，因为应急服务可能在不改变构造的情况下，通过任何SP发起。

这个要求的最终目的是在所有网络（演进的和已存在的）之间建立互通性和互操作性。

7.7 移动性

移动性要求电信基础设施是由可运输的、可重新部署的和完全移动的设施组成。为了具有移动能力，提供应急能力的关键部件应该采用通用构造。电信基础结构应该支持用户和终端的移动性，包括可重新部署或完全的移动通信。随着多数无线终端既支持WiFi也支持蜂窝技术，为增加移动网络中的语音流量进行数据卸载日益重要。应急通信可以是语音或数据，这些卸载能力应为语音和数据业务提供优待处理。

7.8 普遍覆盖

通信资源实现普遍覆盖，即可以为一般大众提供业务支持，也可以成为提供应急通信能力的良好基础。这种情况下，在启动应急作业时就不需要等待部署特殊的设备，因为通信资源信手可得。然而在一些地方，不具备可满足应急通信要求的网络，此时应急通信用户只能获得与一般大众相同的通信能力。

因此，覆盖大范围地理区域的公众电信基础设施，应该成为建设普遍覆盖的应急通信的框架。

7.9 生存能力/抗毁性

支持应急通信的关键网络设施需要尽可能的稳健以抵御灾难。

网络的各种能力也应该很稳健，以支援那些遭受了各种自然或人为灾难，在不同环境中幸存下来的用户。

7.10 语音传输

通常来讲，在应急恢复中的基本通信方式一直是并且今后将仍然是语音通信，因此网络需要为应急作业提供语音传输能力。电路交换网络天生就具备这种能力。而对于分组交换网络来说，需要提供：低抖动、低丢包率以及低时延的，质量可接受的双向实时语音流。电路交换和分组交换网络都需要为应急通信用户保证语音传输质量。

7.11 视频传输

除语音通信外，互动视频通信已成为应急恢复工作中日益重要的手段。在分组交换网中，视频服务可通过相同的针对语音（包括类似信令）的面向会话的参考架构予以传送。然而，视频包括音频和视频部分，可能涉及不同于语音的网络带宽和性能要求，因此与通常的语音采用不同的模式，如双向音频会话和双向视频，或双向音频会话和单项视频。视频用于应急恢复的视频服务可成为服务提供商提供的优先视频会议服务的组成部分。

7.12 数据传输

除语音传输外，无处不在的互联网导致基于包的语音和数据传输能力的提高。许多服务提供商在其管理的数据网络中提供语音、视频和数据通信。该网络为从手持移动终端到住所和企业中固定终端的各项装置提供多媒体通信。这些通信方式为应急通信用户提供了多种选择，既可作为备用通信路径，也可作为通达基础设施受到破坏的区域的备用方法。应急通信的服务质量（QoS）应尽量达到标准。 上述情形中的数据网络应通过低包损耗确保服务质量。

[ATIS-1000057]描述了可用来支持应急恢复工作的两类数据服务：保障速率（GBR）数据服务和数据传送（非GBR）。除此之外，用来支持应急恢复工作的数据服务范围更广，可包括具有优先地位的以下商业服务：万维网服务、文件传送、电子邮件、IP之上的短信服务（SMS）和即时消息（IM）。

广泛使用的电子邮件利用简单邮件传送协议（SMTP）。尽管采用多种方式在冠字字段中表明重要性和优先性，这些方式（方法）通常采用极不相同的句法，因此，SMTP接收机要以不同的方式处理这些情况。然而，可采用标准方式进行消息的提交，邮件消息的提交和传送参考[b-IETF RFC 6409]以及简单邮件传送协议[IETF RFC 5321]参考。但面对两个IETF选择：(1) 在“收到邮件”指令中用一组整数值表明优先等级来确定优先参数，(2) 在通过不支持[IETF RFC 6710] (1)中参数的传送媒介里转接消息时确定SMTP冠字的扩展。尽管优先的实际值和语意取决于相关政策，当授权用户使用SMTP进行应急通信服务时一套数值包含其中。处理优先参数或该方法确定的冠字是当网络节点采用这些扩展部署时可考虑采用的方法。

另一个通信实例是向公民发送有关大规模紧急情况的主管机构告警（如海啸告警和其它自然或人为灾害告警，使用诸如通用告警系统协议[ITU-T X.1303]等机制）。这类通信分两个阶段。在第一阶段中，告警可能基于预订，如向家长发出的学校停课告警或向居住在某一区域的公民发出的有关海啸告警（没有明确预订）。第二阶段涉及可靠的告警传送。

7.13 可变的带宽

在紧急情况下并且电信基础资源即将耗尽时，需要给予应急通信高于一般通信的优先级。一种实现的方法是根据应急通信的需要对带宽进行重新划分，降低一般通信的可用带宽，此时有可能影响到已经建立连接的通话的QoS。在通信资源开始变得不可用时，一般的通信可能会被降级或释放，从而降低了非应急通信业务的服务质量。

用户从运营者那里获得应急通信支持时，可以提出带宽需求。获得授权的用户可选择应急通信能力以支持不同的带宽需求。

7.14 拥塞控制机制中的优待处理

在分组交换网中，许多边缘和核心路由都配置了门限和拥塞控制机制以降低拥塞水平。这些机制可造成正常业务和优先业务的包丢失（取决于拥塞水平）。尽管应急通信可获得高于尽力而为的业务的优先，如将有关机制用于所有业务可能会影响应急通信。这些拥塞控制机制应在配置中确保授权应急通信用户的业务即使在性能降低的情况下继续通信，而不受这些机制的影响。

在提供信令支持时，例如SIP中的资源优先冠字字段，可确定业务类型。标签还包含不同类业务的优先状况。拥塞控制机制应能识别应急通信并例外地减少这些业务的包丢失。紧急业务在拥塞中应比普通业务采用更少的措施。

在下一代移动和固定网中，使用IP多媒体子系统（IMS）将日益重要，特别相对于无线接入网（RAN）而言，如长期演进（LTE）网络。对于移动接入，经授权的应急通信用户的用户设备都配置了接入级超载保护代码，以便在拥塞中的随机接入信道（RACH）获得优先权。基站、MME和包括支持拥塞中超前优先等网信令参数的网关在内的网元在拥塞中为应急通信提供优先权。[ETSI TS 133 401]和[ETSI TS 122 011]描述了有关影响超载保护的安全和接入级别的系统架构。

从服务提供商角度，拥塞中的业务管理经常可使用三种衡量标准：基于速率、基于流量和基于应用。一些限制过低或过高地限制了网络，有关政策影响应用层安全支持（加密）。为使运营商采用与应用无关的的衡量标准并解决性能不确定性，有运营商支持发送者除接收者的拥塞通知反馈外，提供面临拥塞信号。发送者将预期拥塞包含在数据字头之内，而中介节点从字头信息路径中了解到拥塞。运营商可监测这些正常情况下的面临拥塞信号并采取必要的行动以改进应急通信服务（ETS）业务的接通概率。

紧急业务不得受到长时间延迟。举例而言，上文所述现象通过实际测量发现，网络中的大缓冲器造成延迟增加。在拥塞中，这些大缓冲器的影响破坏了拥塞控制的有益性。这些缓冲器在网络各点的配置、监测和管理是确保在延迟可接受的情况下高成功概率的关键。

在管理这些缓冲时，已确定了高效积极地排队管理特性[b-Nichols]。有控制的延迟管理将基于最小的排队规模而非平均排队规模予以考虑，状态变量可跟踪最小排队规模和队伍中剩余的时间包。这些是管理大缓冲器的方法比目前使用的排队规模门限和链路更好。了解排队管理并部署适当的措施，同时增加每跳延迟反弹行为将缓解应急通信业务中的高延迟问题。

应尽力使用不同变量机制，如标准化QoS来设计和维护网络。

7.15 可靠性/可用性

为了实现效用最大化，应急通信应该是即可靠又可用的。如果可行，就通过权限控制和网络策略为应急通信提供优先权处理，以提高通信的成功率。

包括硬件、软件和其他电信资源在内的所有内容与设计要求和规范保持一致，并且在使用上应该是高度可信的，符合服务水平协议规定。

服务水平协议（SLA）提高了ETS客户的信心，是他们设计了服务提供商网络必须遵守的要求和规范。

远程管理论坛（TMF）SLA管理手册[b-TMF GB917]规定了用来在客户和服务提供商之间制定SLA的标准方法，该手册使用了服务水平规范（SLS）概念，确定包含SLA的可衡量参数。SLS用来定义纳入SLA的关键质量指标（KQI）参数以及相关门限值，亦建议使用诸如[ITU-T M.3342]规定的模板。

在TMF SLA手册中，制定SLA规范被视为“业务流程”。该业务流程进一步分解为更低层面的业务流程，其中包括：

- 捕获SLA要求
- 编写SLA草案
- 核对SLA完整性
- 认证SLA规范
- 签署SLA规范。

各业务流程的详细使用说明分别针对客户和服务提供商。显示这些业务流程适用于具体服务情形（如ETS）的实例（所谓“使用案例”）亦涵盖其中。

更深入的实例（所谓“应用说明”）见其它文件。举例而言，[b-TMF GB934]是一个旨在说明IP语音SLA管理的应用说明。[b-TMF GB934]亦包含有关ETS状况下IP语音的SLA管理讨论。相对于公共服务，ETS的主要区别之一是强调在非正常（如超载）条件下的KQI。

为达到网络可用性和可靠性要求，可使用[b-TMF GB917]和[b-TMF GB934]中的ETS实例，特别用于有关语音服务的讨论[b-TMF GB934]。其它有关ETS的SLA管理工作正在进一步研究中以便应对数据和视频KQI的开发。

7.16 ETS对云基础设施的使用

[ITU-T Y.3501]提供了通用的云计算要求和能力。本建议书附件A包含应急通信的功能要求和能力清单。在应急通信中需要对这些要求予以支持，其中包括云服务提供商（CSP）提供的ETS（[ITU-T Y.3510]）。

目前定义的云计算基础设施可用于服务提供商（如NGN提供商）对公众网络服务的支持，如包括ETS的应急通信。如云计算基础设施用来支持包括ETS在内的应急通信，本建议书规定的网络资源和核心传送网络应急处理要求将适用并应包含在内。举例而言，在灾害和紧急状态下，ETS向ETS授权用户提供优先通信。对于云资源管理，如云基础设施用来支持公众网络服务，经授权的ETS用户应得以获得云资源的优先权（如优先处理）。此外，本建议书规定的应急通信要求适用于[ITU-T Y.3501]和[ITU-T Y.3510]规定的云参考架构的多个层面。

[ITU-T Y.3520]提供了有关端对端云计算资源管理要求的一般性概念。如云计算资源用来支持ETS，根据[ITU-T Y.3520]，有必要采用适当的资源管理功能，以便在授权用户使用云计算资源时得到优先处理。

[ITU-T Y.3510]附件IV提供了有关对ETS使用云基础设施资源的指导和详情。该附件与本建议书规定的网络资源和核心传输网络要求相关。

附件 A

基本要求和可选要求之间的可能区别

（此附件是本建议书不可分割的组成部分）

应急通信功能 要求和能力	描述	基本要求	可选要求
增强的优先权处理	应急通信业务在穿越任何网络时都需要获得保障	X	
安全的网络	网络应该在业务和控制中适当地使用扩展的加密技术和用户授权，以防止欺骗和未授权的接入。	X	
位置保密	少数处于高级领导层的应急通信用户在组织应急减灾行动时，决不能面临位置被发现的风险。		X
可恢复性	电信网络应该有能力被完全修复，或至少被恢复到能支持优先通信的水平。		X
网络连通性	在可能的情况下，支持应急通信的网络应该提供国际互连性，如能应用[ITU-T E.106]和[ITU-T E.107]建议书时。	X	
协同工作能力	在所有网络（演进的和已存在的）之间建立互通性和互操作 能力	X	
移动性	电信基础结构应该支持用户和终端的移动性，包括可重新部署或完全移动的通信。	X	
普遍覆盖	覆盖大范围地理区域的公众电信基础结构，应该成为建设普遍覆盖的应急通信的框架。	X	
生存能力/抗毁性	网络能力应该很稳健，以支援各种环境中幸存下来的用户。	X	
语音传输	电路交换和分组交换网络需要为应急通信用户提供语音频带的高质量服务。	X	
视频传输	电路交换和分组交换网络应为应急通信用户提供具有低包误差率和丢失的语音频段高服务质量。	X	
数据传输	分组交换网络应为应急通信用户提供低包误差率服务质量。	X	

应急通信功能 要求和能力	描述	基本要求	可选要求
可变的带宽	获得授权的用户可选择应急通信能力以支持不同的带宽需求。		X
可靠性/可用性	通信系统应该与设计要求和规范保持一致，并且应该是高度可信的。	X	
拥塞控制机制中的优待处理	拥塞控制机制应支持应急通信业务比普通业务更少受到措施限制，		X

附录一

关于灾难可能来源的信息

（此附录不构成本建议书不可分割的组成部分）

两种形式的力量引发了大多数的自然灾害事件。它们是：极端的天气条件（暴风雨）和地震。它们都会释放难以预知的能量并在不同的地理范围内造成不同程度的破坏。飓风（通常提及的台风和龙卷风）会席卷很大范围的地理区域并且是地球上最具破坏性的极端天气条件。由暴风雨天气产生的风雨及二次效应（比如洪水），会对财产和生命安全造成广泛的和持续的破坏。虽然暴风雨的很多方面（比如强度和经过路径）能够被预报，也能为人们提供一个预警期，但是对财产和土地的破坏仍然会发生。与极端的天气情况相反，地震在很大程度上难以预测，但是却限制在一个很小的地理范围之内。大自然的威力时常会显现，并对财产和生命安全造成巨大破坏，特别是在世界上人口稠密的地区。

通常，自然灾害会引发其他事件。举例来说，飓风可能会导致山洪暴发或泥石流。飓风还可能引起河流泛滥，导致家畜死亡和农田遭受破坏。人们会面临断电或者失去家园，使得他们需要食物、衣服和避难所。地震过后，余震会持续的造成破坏。一些地震会引发海潮，对已经受灾的地区造成额外的伤害。近来，一些灾害连续发生，使规划内应对灾害的措施面临挑战。地震可能会引发核设施影响以及在规划响应措施时从未设想或考虑到的一系列问题。

部分自然灾害被列举请参见表I.1：

表 I.1 – 自然灾害

雪崩
干旱
地震
流行病
山洪爆发
饥荒
洪水
森林火灾
雷击
飓风
泥石流
严寒、雪灾、冰雹或炎热
海潮
龙卷风
海啸
台风
火山爆发
风暴

由人类滋生的灾难事件在能量、地理分布、持续时间和损害程度上也是不相同的。

人类引起的灾难可以与自然界相匹敌。和自然灾害一样，它们也会从原始事件中衍生出其他事件。比如，煤矿着火会导致因灼烧和烟雾吸入失去生命。这种火灾除了会坑害矿井里的人员，还会引起其他爆炸。表I.2列出了人类引起的灾难。

表 I.2 – 人为灾难

纵火
化学泄漏
工业或国家体系崩溃
爆炸
火灾
气体泄漏
核爆炸
管道破裂
飞行器坠落/紧急迫降
投毒
放射污染
船只碰撞/翻覆
（牛群、马群）惊跑
地铁碰撞/出轨
恐怖袭击
火车碰撞/出轨
由水引起的事故

参考资料

[b-IETF RFC 5559] IETF RFC 5559 (2009), *Pre-Congestion Notification (PCN) Architecture*.

[b-IETF RFC 6409] IETF RFC 6409 (2011), *Message Submission for Mail*.

[b-Nichols] Nichols, K., Jacobson, V. (2012) *Controlling Queue Delay*. *Association for Computer Machinery*.
<http://queue.acm.org/detail.cfm?id=2209336>

[b-TMF GB917] TMF GB917 (04/2012), *SLA Management Handbook Release 3.1*.

[b-TMF GB934] TMF GB934 (06/2008), *Application Note to SLA Management Handbook, Release 2.0*.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目和其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	**全球信息基础设施、互联网的协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2014年，日内瓦