International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.1271

(07/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Architecture, access, network capabilities and resource management

Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks

Recommendation ITU-T Y.1271

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	**Y.1200–Y.1299**
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.1271

Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks

Summary

Many challenges and considerations need to be addressed in defining and establishing the functional capabilities to support emergency telecommunications in evolving circuit- and packet-switched telecommunications networks. This Recommendation presents an overview of the basic requirements, features, and concepts for emergency telecommunications that evolving networks are capable of providing.

History

Edition	Recommendation	Approval	Study Group	Unique 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

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

The purpose of emergency telecommunications is to facilitate emergency recovery operations with the goal for restoring the community infrastructure and for returning the population to normal living conditions after serious disasters. In some countries, emergency recovery operations are considered to fall within the scope of public safety organizations. Responders need to assess the damage, coordinate rescue and medical assistance, harmonize restoration endeavours, etc. For supporting this purpose, emergency telecommunications may be provided through shared resources from the public telecommunications infrastructure, and in some cases through additional resources of enterprise networks (e.g., the public safety network), that are evolving from a basic circuit-switched to packet-switched networks with a variety of telecommunication capabilities.

Recommendation ITU-T Y.1271

Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks

1 Scope

Contextual understanding and careful thought is required to address the unique challenges faced by emergency telecommunications. This Recommendation presents an overview of the basic requirements, features, and concepts for emergency telecommunications that evolving telecommunication networks are capable of providing. This Recommendation provides guidance to telecommunication network operators on network requirements and capabilities to support emergency telecommunications offerings and to provide responders (users) with useful information for (acquisitions) request of such capabilities.

NOTE – This Recommendation defines requirements for networks which when implemented should help support emergency telecommunication services and facilitate the application of [ITU-T E.106] and [ITU-T E.107] if needed.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[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 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Emergency Telecommunications Service (ETS) [ITU-T E.107]: A national service providing priority telecommunications to the ETS authorized users in times of disaster and emergencies.

3.1.2 next generation network (NGN) [ITU-T Y.2001]: A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 assured capabilities: Capabilities providing high confidence or certainty that critical telecommunications are available and perform reliably.

3.2.2 authentication: The act or method used to verify a claimed identity.

3.2.3 authorization: The act of determining if a particular privilege, such as access to telecommunications resource, can be granted to the presenter of a particular credential.

3.2.4 authorized emergency telecommunication user: A person or an organization authorized to obtain premium privileges and capabilities in national and/or international emergency situations.

3.2.5 bottom-up emergency declaration: An emergency declaration determined or assumed by individual users. The user or users would then use emergency telecommunications according to individual authorizations or authorities.

3.2.6 buffer-bloat: A situation in a packet-switched network whereby large buffers at various network nodes and end systems cause excessive latency and jitter, as well as reduce the overall network performance. This situation may affect how quickly emergency situations are communicated.

3.2.7 confined emergency situation: An emergency situation within a certain defined relatively small geographic area (e.g., local) not affecting other areas.

3.2.8 declared emergency situation: An emergency publicly recognized and stated by a responsible authoritative official(s) of the responsible government(s).

3.2.9 emergency situation: A situation, of serious nature, that develops suddenly and unexpectedly. Extensive immediate important efforts, facilitated by telecommunications, may be required to restore a state of normality to avoid further risk to people or property. If this situation escalates, it may become a crisis and/or disaster.

32.10 international emergency situation: An emergency situation, across international boundaries, that affects more than one country.

3.2.11 label: An identifier occurring within or attached to data elements.

3.2.12 nationwide emergency situation: An emergency situation that affects an entire nation, but remains confined in scope to only one country.

3.2.13 ordinary emergency capability: A special emergency type of telecommunications capability (such as 911, 110, or 112) used on a national level made available to the general public to report local or personal emergencies to government officials or other officially designated civil authorities.

3.2.14 policy: Rules (or methods) for allocating telecommunication network resources among types of traffic that may be differentiated by labels.

3.2.15 precedence: When a privilege exists to enable, or facilitate, the preceding of others.

3.2.16 preferential: A capability offering advantage over regular capabilities.

3.2.17 preferential treatment in congestion control mechanisms: Methodologies to manage telecommunication resources to minimize the impact of congestion on emergency telecommunications. Congestion can be managed via a number of measures, such as network design, network element mechanisms (e.g., machine congestion controls) and network operational capabilities.

3.2.18 priority treatment capabilities: Capabilities that provide premium access to, and/or use of telecommunications network resources.

3.2.19 public safety: An umbrella term used in some regions to encompass emergency recovery operations along with other services such as fire and rescue, ambulance and emergency medical services, police and security guard licensing services, etc. for the welfare and protection of the general public. The primary goal is prevention, and protection of the public from dangers affecting safety such as crimes or disasters.

3.2.20 top down emergency declaration: When responsible official(s) with recognized authority in Government, or industry issue an emergency declaration.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CSP Cloud Service Provider

DSL Digital Subscriber Line

ETS Emergency Telecommunications Service

GBR Guaranteed Bit Rate

IM Instant Messaging

IMS IP Multimedia Subsystem

KQI Key Quality Indicator

LTE Long Term Evolution

NGN Next Generation Network

QoS Quality of Service

RACH Random Access Channel

RAN Radio Access Network

SLA Service Level Agreement

SLS Service Level Specification

SMS Short Message Service

SMTP Simple Mail Transfer Protocol

SP Service Provider

5 Security

Due to the nature of this Recommendation, security is addressed in general. However, special attention should be given to clause 6.3 and clause 7 where several requirements may have strong security implications, such as authorization (clause 6.3), network integrity (clause 7.2), secrecy aspects of selected users (clause 7.3), network restorability (clause 7.4), interoperability (clause 7.6), survivability/endurability (clause 7.9) and reliability/availability (clause 7.15). Other ITU-T Recommendations may complete this Recommendation with regard to security aspects.

6 Consideration

6.1 The nature of emergency situations

Disasters often happen as sudden events that cause immense damage, loss and destruction. Disaster events occur due to the forces of nature or because of actions that stem from human sources or interventions. Disasters can have extreme magnitude, be long lasting, and cover wide geographic areas within national or international boundaries. In other words, disasters are variable in magnitude (energy), duration (time) and geographic area.

Hundreds of disasters occur each year all over the world; no country is immune. A confined disaster may be quite severe and yet by definition is local in nature. Disasters may affect an entire region, such as with nationwide or international emergency situations. Each disaster brings suffering, financial and social consequences. Regardless of the kind of disaster, telecommunications are needed to respond effectively and save lives.

In most countries plans and measures (e.g., tests, exercises and drills) are designed and deployed to anticipate and effectively address disasters. However, sometimes a scenario known as "black swan" may occur. An unusual combination of abnormal conditions may challenge or defy traditional disaster anticipation and mitigation.

6.2 Emergency response

All types of disasters, whether attributed to natural or human sources, can strike anywhere and at any time. Disaster recovery occurs in stages. The first responders to a disaster scene play the primary role in assessing and containing the damage. Other phases follow in quick succession. In the second phase the injured are treated and the saving of lives is priority. The third stage often brings additional disaster recovery personnel, equipment and supplies, perhaps from pre-positioned sites, storage facilities or staging areas. The fourth phase comprises clean-up and restoration.

The common thread to facilitate operations for all disaster recovery phases is the utility of fast, reliable, user-friendly emergency telecommunications that may be realized by technical solutions and/or administrative policy. It should be realized that some of the existing plans initially accounted for adversities that were greater than these response measures – for example, earthquakes may be stronger than the measures that were planned for them.

6.3 Assured telecommunications

The goal is assured telecommunication capabilities during emergency situations. Disasters can impact telecommunications infrastructures themselves. Typical impacts may include: congestion overload and the need to re-deploy or extend telecommunications capabilities to new geographic areas not covered by existing infrastructures. Even when telecommunications infrastructures are not damaged by the disaster, demand for telecommunications soar during such events.

The method by which authorities are notified of an emergency situation varies widely. Citizens using an ordinary emergency capability may notify authorities of a disaster. Alternatively, emergency workers that are directly or indirectly interacting with people in the disaster area may make a bottom-up emergency declaration. This information may result in an authoritative official(s) of the responsible government issuing a declared emergency. The latter represents a top down emergency declaration.

The affiliation of an emergency worker may be known in advance of an actual emergency situation. In this case, their credentials may be stored thereby allowing the person to be authenticated for an authorized telecommunication. Generally, when preferential or priority treatment telecommunication capabilities (e.g., to enable precedence over other users) are offered, users of the service need to be authorized and authenticated. Whether authorization is required shall be national matters of the respective particular country. However, without authorization, preferential treatment capabilities may be subject to abuse by non-authorized individuals. Technical considerations for security are discussed in clause 11 of [ITU-T Y.2205].

Circuit-switched and some packet-switched (next generation network [NGN]) networks respond to overload situations by denying call attempt when resources are saturated. Some networks will provide preferential treatment to call requests. One option is to pre-empt other callers when authorized emergency communication workers need to communicate. However, some types of packet-switched networks respond to additional load by degrading performance of individual user traffic in the entire network. This occurs when networks operate under a best-effort framework where all information is treated the same and simply queued or dropped until network resources are available.

Recent studies and measurements indicate that a phenomenon referred to as "buffer-bloat" may introduce unacceptable latency. The reduction in cost of memory has resulted in network resources (including end-user equipment in broadband networks) having large buffers. These buffers result in delaying timely congestion notifications that are meant to minimize the impact of congestion. These

large buffers may impact not only the best-effort traffic, but also priority traffic such as that of emergency telecommunications.

Providing a preferential treatment to emergency telecommunications and by providing fault tolerant networks that will not fail because any one component fails are important steps toward assured capabilities. While fault tolerant networks are a critical step toward assured capabilities, telecommunications network operators should also maintain recovery plans to restore networks in the event of failure.

7 Emergency telecommunications requirements and capabilities

Fully comprehensive emergency telecommunications need to have many capabilities to support a variety of operational requirements for emergency recovery forces. Table 1, as shown below, lists specific objectives and requirements that could potentially facilitate telecommunications for disaster recovery activities. Implementing these requirements into operational capabilities greatly facilitates effective and timely recovery operations during emergency events.

NOTE – Where solutions to such requirements are implemented, they could also be used to support ordinary emergency services like traditional 110, 112, 911 and so on. Requests to meet particular requirements and the conditions thereof shall be national matters of the respective country.

Table 1 provides objectives and functional requirements.

Table 1 – Emergency telecommunications functional requirements and capabilities

Enhanced priority treatment
Secure networks
Location confidentiality
Restorability
Network connectivity
Interoperability
Mobility
Ubiquitous coverage
Survivability/endurability
Voice transmission
Video transmission
Data transmission
Scaleable bandwidth
Reliability/availability
Preferential treatment in congestion control mechanisms

7.1 Enhanced priority treatment

Emergency telecommunication traffic needs assured capabilities regardless of the networks traversed. A prime component of assured capabilities is enhanced priority treatment. One potential method to achieve priority treatment is to first "identify" (e.g., classify and/or label) emergency traffic and then apply network policy to this traffic in order to achieve the desired assured service. In connection-oriented transport, once a connection is established, the call effectively is "hard wired", has guaranteed performance and does not necessarily require continuance of preferential status. With connectionless packet-switched transport, however, it may be necessary to maintain the emergency telecommunication identification for each packet. Telecommunication network operators and service providers (SPs) need to be able to identify and prioritize emergency telecommunications according to their SLA with users.

New or temporary emergency operations users require a network operator to provision an access line[1]. It is desirable for provisioning to occur on a preferential basis to enable rapid initiation of emergency telecommunications.

7.1.1 Preferential access to telecommunications facilities

There are a number of ways to access telecommunication resources for obtaining emergency telecommunication capabilities. These include analogue subscriber line, wireless, satellite, cable, digital subscriber line (DSL), and optical fibre. There will be a significant advantage for an emergency operations user to be able to obtain access to these various telecommunications network services on a priority or preferential basis. This will enable more rapid initiation of emergency telecommunications.

The traditional circuit-switched network regularly has no general provision for signalling priority access requests. However, specially marked lines or specifically provisioned "off-hook" services could provide preferential access, but that would only be by line and location and not per emergency telecommunication request. There is currently no provision for conveying a priority dial tone or service initiation via general access from a conventional telephone instrument. A dial tone comes on a demand basis from a limited selection of ports and heavy traffic conditions can delay access if demand consumes the supply of ports. Therefore, a provision for preferential access to services in evolving networks is a capability that requires consideration.

7.1.2 Preferential establishment, use of remaining operational resources and completion of emergency traffic

Emergency traffic needs to be identified in order to distinguish this type of traffic with respect to ordinary traffic. With traditional circuit-switched networks, only the signalling protocol is able to distinguish the two traffic types. However, in packet-switched networks, identification through the use of labels in either signalling or data elements can facilitate distinguishing types of traffic. In packet-switched networks, labels can reside in different layers or sublayers.

Once traffic is identified, telecommunication network policy rules or methods should be applied to provide an enhanced priority treatment to emergency traffic. With connection-oriented transport, the policy potentially includes a higher probability of call admission. With connectionless oriented transport, the policy needs to provide a higher probability of success relative to the success of the routing and delivery of ordinary traffic.

7.1.2.1 Completion of emergency traffic during congestion

Emergency traffic needs to be minimally impacted during network congestion. Traditional circuit-switched networks applied traffic control methods such as call blocking to reduce congestion on the networks. Emergency traffic is distinguished by minimizing blocking and ensuring a high probability of call completion over normal traffic.

In packet-switched NGN, priority signalling, priority transport of signalling and media and various preferential treatment mechanisms (including congestion control mechanisms) for emergency traffic are used to prevent blocking and ensure a high probability of completion of emergency traffic, as compared to normal traffic.

7.1.2.2 Exemption from network management controls

Based on regional/national requirements and network operator policy, emergency telecommunications should be exempted from network management controls up to the point where further exemption would cause network instability. Congestion controls (e.g., machine congestion

[1] If access line is used in this context, it means a wired as well as wireless access, channel, virtual connection, tunnel, etc.

controls), overload controls and load balancing should not adversely impact emergency telecommunications.

7.1.3 Preferential routing of emergency telecommunication traffic

In some situations, emergency traffic could be redirected to alternate paths when default paths have become unusable or congested. In evolving networks, it is desirable for emergency telecommunications to avoid single points of failure and hence possibly have multiple backup paths or alternate routing for use during periods of overload or failed connections through the network. In packet-based networks, routing of packets is a continuing process for an instance of telecommunication until the session has reached completion. As a result, the traffic monitoring and network controls should be continuous to avoid the impacts of overloaded connections and systems. In addition, the effect of large buffer overloads may shift across the different elements of the network with the variation of available actual bandwidth. Thus constant monitoring and controls are required to manage the buffers and avoid high latency for the emergency traffic.

In addition, several new congestion avoidance techniques (as opposed to congestion control) have emerged in recent years that can be deployed to support users of emergency telecommunications [IETF RFC 4412], [b-IETF RFC 5559], [IETF RFC 5670] and [IETF RFC 6679].

7.1.4 Optional pre-emption of non-emergency traffic

While the concept of pre-emption typically applies to circuit-switched communications, its application in some packet-switched (NGN) networks is also defined. Pre-emption of non-emergency traffic to free bandwidth and resources for emergency traffic is an optional requirement; the basic emergency telecommunications provisions do not include the concept of pre-emption. However, using labels to prioritize emergency traffic is one approach to identify and make available resources for emergency traffic over normal traffic.

7.1.5 Allowable degradation of service quality for traffic, as infrastructure resources become unavailable

The QoS for different modes of service for the emergency telecommunications would typically be designated as the best available to ensure clear clean telecommunications and conveyance of important information. However, when the telecommunication resources are experiencing severe stress, an allowable degradation of QoS may be acceptable. This could occur only when resources have become unavailable to the point that the network cannot support non-emergency traffic and sufficient bandwidth and resources are not available to support the normally acceptable QoS level for emergency traffic. Rather than lose the ability to communicate, emergency operations need to continue to convey critical information, even if constrained.

In justified cases during declared emergency situations where telecommunications infrastructure resources are leading to exhaustion, then it may be necessary to give emergency telecommunications priority over the ordinary telecommunications. This may affect established telecommunications in terms of QoS. As a result, ordinary telecommunications in progress may be degraded or released.

7.2 Secure networks

Security protection is necessary to prevent unauthorized users from obtaining scarce telecommunication resources needed to support emergency operations.

7.2.1 Rapid authentication of authorized users for emergency telecommunications

The emergency telecommunications is intended only for authorized users who participate in emergency recovery operations. The appropriate authority of each nation or community may authorize these designated users. Upon initiation of an emergency communication request, for evolving networks, it is desirable to request to establish an innovative method for a streamlined rapid user authentication process in these evolving telecommunication networks, including mobile

networks which verifies the user's identity to protect the telecommunication resources against excessive use and abuse during an emergency situation. Once an authentication is validated and emergency telecommunication travels across networks, such authentication information may be associated with labels that then should be transported from the call initiation until termination. It may be necessary for the label to remain throughout the duration of the emergency call.

7.2.2 Security protection of emergency telecommunication traffic

In addition to authentication and authorization, other aspects of security such as measures against spoofing, intrusion and denial of service are required for emergency telecommunications. It is desirable to offer assurance that unauthorized modifications of objects may be detected. Ordinary telecommunications may then also benefit from increased protection from intrusion and denial-of-service attacks. Networks should have protection against (fraud) corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.

7.3 Location confidentiality

For certain emergency telecommunications, special additional security measures may apply. For example, in one potential destructive scenario is the trial to obstruct disaster recovery operations themselves. In such a scenario, emergency telecommunications from selected users need to be protected from manipulation, interception or obstruction by others, due to their urgent and important nature. Special security mechanisms to prevent the identification of the location of certain authorized users of emergency telecommunications from being revealed to non-authorized parties should apply in order to protect such authorized users from being located. These special security requirements are beyond the scope of this framework Recommendation.

A limited number of high level leadership emergency telecommunications users may need to organize emergency relief operations without risk of their location being discovered.

7.4 Restorability

If network capabilities key to emergency operations fail, those capabilities need to be restored in a timely fashion. Both circuit- and packet-switched networks typically require a physical access line, wired or wireless, that extends to customer locations. When access lines are damaged, network operators restore operations but access disruption times may be lengthy. Therefore, it is necessary for restoration to occur on a preferential basis to enable rapid initiation of emergency telecommunications for users of these capabilities.

Should a disruption occur, telecommunication network functionalities should be capable of being reprovisioned, repaired, or restored to required levels on a priority basis.

7.5 Network connectivity

It is advisable that networks supporting emergency telecommunications be connected to other networks thereby providing a wide reach. Interworking preferential treatment at reference points that are deemed to constitute international and/or regulatory boundaries between national networks that provide emergency telecommunications may create international emergency systems, e.g., when [ITU-T E.106] and/or [ITU-T E.107] is applicable.

NOTE – Disaster situations are often regional but may include multiple nations. In these cases, disaster recovery emergency telecommunications from multiple nations may be necessary to respond to one specific event. Also, in the "increasingly networked world", many nations often provide support for recovery operations for emergency disasters contained within the borders of a stricken country.

In certain liberalized and competitive environments, there may be:

a) more than one network operator in a given country;

b) network operators whose networks span more than one country.

In these cases, consideration needs to be given to the interconnection of emergency telecommunications capabilities between network operator boundaries and/or across reference points which constitute national and/or regulatory boundaries.

7.6 Interoperability

Evolving networks will produce a number of issues, one of which is to ensure orderly and transparent continuance of the basic ITU-T E.106 emergency preference capabilities. During the convergence period, the different schemes for interworking between the circuit-switched and packet-switched technologies need to be considered. For example, voice calls from the telephone or mobile network may transit packet-switched networks and then terminate in either the circuit-switched network or directly in a packet-switched network. Interworking requirements for preferential treatment methods over heterogeneous networks have been addressed for PSTN and IPCablecom networks in clause 6 of [ITU-T J.261] and clause 6.2 of [ITU-T J.260]. These requirements may also be applied to other heterogeneous networks.

Configuration issues are often a major cause of interoperability problems. In order to have interoperable capabilities among different operators offering emergency telecommunications, a common configuration will be helpful. Note this does not imply operators must all configure their internal networks the same if they are to support emergency capabilities. It only implies they will translate appropriate configurations at the appropriate ingress/egress locations. This method also allows more ubiquity because any emergency service may be initiated with any contracted SP without configuration modification.

The goal of this requirement is to provide interconnection and interoperability among all networks (evolving or existing).

7.7 Mobility

Mobility calls for a telecommunications infrastructure that is integrated with transportable, re-deployable and fully mobile facilities. In order to have mobile capabilities, a common configuration provides key elements to facilitate capabilities for emergency applications. The telecommunications infrastructure should support user and terminal mobility including re-deployable, or fully mobile telecommunications. With most wireless terminals supporting both WiFi and cellular technologies, data off-loading to enable increased voice traffic on mobile networks is gaining importance. The emergency traffic may be voice or data and these off-loading capabilities should provide preferential treatment to both voice and data traffic.

7.8 Ubiquitous coverage

Ubiquitous telecommunications resources that provide support to services of the general population may provide the basis for readily available capabilities for emergency telecommunications. Because these capabilities are at hand, emergency operations activities do not need to wait for deployment of special facilities. However, in situations where networks do not (or may not) support emergency communication requirements/capabilities, then emergency communication users will default to communication capabilities available to the general public.

Therefore, public telecommunication infrastructure resources over large geographic areas should form the framework for ubiquitous coverage of emergency telecommunications.

7.9 Survivability/endurability

Key network infrastructure supporting emergency telecommunications needs to be as robust as possible so as to endure throughout the disaster.

Capabilities should be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or human-made disaster.

7.10 Voice transmission

Traditionally, the fundamental telecommunications method for emergency recovery has been and will continue to be voice communications. Hence, networks need voice transmission capabilities for emergency operations. Circuit-switched networks provide this by default while packet-switched networks require support of: low jitter, low loss and low delay for acceptable interactive real time voice media streams. Circuit-switched and packet-switched networks should provide voice transmission quality service for emergency telecommunications users.

7.11 Video transmission

In addition to voice communications, interactive video communications are becoming an increasing important tool for emergency recovery operations. Within packet-switched networks, video services can be delivered over the same session-oriented reference architecture used for voice, including similar signalling. However, video includes audio and video components that may involve very different network bandwidth and performance requirements from that of voice, and may be used in different modes from those generally thought of for voice, e.g., two-way audio conversations with two-way video, or two-way audio conversations with one-way video. Video services used for emergency recovery could become part of a priority video conferencing service offered by a service provider.

7.12 Data transmission

In addition to voice transmission, the fundamental, ubiquitous presence of Internet has resulted in increasing packet based voice and data transmission capabilities. Many service providers offer voice, video and data communications over their managed data network that provide for multimedia communications to various devices ranging from hand-held mobile terminals to fixed terminals located in residences and enterprises. These communication methods offer more choices for emergency telecommunications users both as alternative paths of communication and alternative methods to reach areas that may have damaged infrastructure. The Quality of Service (QoS) for emergency telecommunications, based on the standards, should be maintained as much as possible. The QoS in terms of minimum loss of packets should be provided by the data networks in such a scenario.

[ATIS-1000057] describes examples of two types of data services that may be used to support emergency recovery: guaranteed bit rate (GBR) data service, and data transport (non-GBR). In addition to these, the broader family of data services used in support emergency recovery operations may include prioritized versions of the following commercial services: web service, file transfer, e-mail, short message service (SMS) over IP and instant messaging (IM).

For e-mail, a widely used method involves using the Simple Mail Transfer Protocol (SMTP). Even though different approaches have been used to indicate in the header fields such as importance and priority, these approaches (methodologies) often present widely varying syntax, and consequently, SMTP receivers deal with these approaches differently. Nevertheless, a standard approach may be applied during message submission: reference Message Submission for Mail [b-IETF RFC 6409], and reference Simple Mail Transfer Protocol [IETF RFC 5321] for transfer, but with two IETF options as follows: (1) by defining a priority parameter in the "Mail From" command with a set of integer values designating the priority level, and (2) by defining an extension to the SMTP header which is used when relaying a message through transfer agents that do not support the parameter discussed in (1) [IETF RFC 6710]. Even though the actual values and semantics of the priority depend on the policies in place, an example set of values are included for the case when a set of authorized users use SMTP to communicate emergency telecommunications services. The principles for handling the priority parameter or header defined by this approach may be considered for adoption as the nodes of the network are deployed with these extensions.

Another data communications example is the need to exchange alerts from authorities to citizens related to large-scale emergencies such as tsunami warnings and other natural or man-made disasters using mechanisms such as a common alerting protocol [ITU-T X.1303]. There are two phases present in this type of communication. In the first phase, the alerts may be subscription based such as school closures sent to parents, or sent to those residing in a specific geographic area as in the case of tsunami warnings without an explicit subscription. The second phase relates to the reliable delivery of alerts.

7.13 Scaleable bandwidth

In justified cases during declared emergency situations where infrastructure resources are leading to exhaustion, then it may be necessary to give emergency telecommunications priority over the ordinary telecommunications. One method to achieve this is to allow emergency telecommunications scalable bandwidth to enable reducing the bandwidth available for ordinary telecommunications and thus potentially affect established telecommunications in terms of QoS. Ordinary telecommunications may be degraded or released thereby to an allowable degradation of service quality for non-emergency telecommunication traffic, as infrastructure resources become unavailable.

Broadband is a user requirement that may be requested during acquisitions of emergency telecommunications from operators. Authorized users should be able to select the capabilities of emergency telecommunications to support variable bandwidth requirements.

7.14 Preferential treatment in congestion control mechanisms

In the case of packet networks, many of the edge and core routes are configured with thresholds and congestion control mechanisms to reduce the level of congestion. These mechanisms result in dropped packets for both normal and priority traffic depending on the level of congestion. Even though the emergency telecommunications may be given a higher priority than best-effort traffic, the mechanisms, if applied to all traffic, may throttle emergency telecommunications. These congestion control mechanisms should be configured such that authorized emergency telecommunication users' traffic continues to communicate even at a degraded level without being subject to these mechanisms.

When signalling support is available, for example, the resource priority header field in SIP, the types of traffic can be identified. Labels are also included to distinguish the priority of different types of traffic. The congestion control mechanisms should be able to recognize the emergency traffic and offer exemptions to minimize dropped packets for such traffic. Emergency traffic should have reduced measures applied compared to normal traffic during congestion.

In next generation mobile and fixed networks, the use of an IP multimedia subsystem (IMS) has gained importance, especially with respect to radio access networks (RANs) such as long-term evolution (LTE) networks. For mobile access, the user equipment for authorized emergency telecommunication users is configured with an access class overload protection code to gain priority access on the random access channel (RACH) during congestion. Network elements such as base station, MME and gateway support signalling parameters (such as advanced priority) during congestion to provide prioritization of emergency telecommunications during congestion. [ETSI TS 133 401] and [ETSI TS 122 011] describe evolving 3GPP system architecture for security and the access class barring overload protection, respectively.

From the service provider's perspective three metrics are commonly used to manage traffic in the presence of congestion: rate-based, volume-based and application-based. Some of the limitations of these approaches include over or under constraining the network and policy concerns resulting from application-layer security support (encryption). In order for the operator to perform the application agnostic metric and overcome performance uncertainty, there is support from operators for the sender to provide congestion exposure signals in addition to congestion notification feedback from the receiver. The sender includes expected congestion in the header of the data and the intermediate nodes learn about the congestion on the path from the header information. The operator can monitor these

exposure signals specifically under abnormal conditions and take the necessary action to improve the probability of completion for Emergency Telecommunications Service (ETS) traffic.

Emergency traffic should not experience high latency. For example, the phenomenon described above that has been found by actual measurements is the increased latency resulting from large buffers in the network. During congestion, the impact of these large buffers negates the usefulness of the congestion control. Configuring, monitoring and managing these buffers at all points in the networks are crucial to have a high probability of success with acceptable latency.

In managing these buffers, certain characteristics that are important for efficient active queue management have been identified [b-Nichols]. A controlled delay management is to be considered based on minimum queue size instead of average queue size, a state variable to track the minimum queue size and the time packet remaining in the queue. These are considered to be better measures to manage large buffers than, for example, thresholds on queue size and link utilization that are used currently. Understanding queue management and deploying appropriate measures combined with delay-bound per-hop behaviour are likely to mitigate high latency for emergency telecommunications traffic.

The networks should be designed and maintained, using various available mechanisms, such that the standardized QoS is maintained as much as possible.

7.15 Reliability/availability

To provide the greatest utility, emergency telecommunications need to be both reliable and available. Whenever possible, admission control or network policy can increase the probability of successful telecommunications by providing a preferential treatment to emergency telecommunications.

All components that encompass hardware, software and other resources of telecommunications should perform consistently and precisely according to their design requirements and specifications, and should be usable with high confidence – in accordance with service level agreements (SLAs).

SLAs may assist in giving the ETS customer confidence that design requirements and specifications have been adhered to within the service provider's network.

TeleManagement Forum's (TMF's) SLA Management Handbook [b-TMF GB917] specifies a formal methodology that may be used to develop SLAs between customers and service providers. The Handbook utilizes the concept of service level specification (SLS) to identify measurable parameters for inclusion with an SLA. The SLS is used to define key quality indicator (KQI) parameters, along with associated threshold values, for inclusion within an SLA. The use of SLA templates such as those specified by [ITU-T M.3342] is also recommended.

Within TMF's SLA Handbook, development of an SLA specification is considered to be a "business process". This business process is further decomposed into lower level business processes that include:

- capturing SLA requirements;
- preparing draft SLA;
- checking SLA completeness;
- validating SLA specification;
- signing-off SLA specification.

The use of each business process is explained in detail from both a customer and a service provider perspective. Examples (referred to as 'use cases') showing how these business processes may be applied in the context of specific services (e.g., ETS) are also included.

More in-depth examples, referred to as "application notes", are typically produced as separate documents. For example, [b-TMF GB934] is an application note dedicated to voice over IP SLA management. [b-TMF GB934] also includes a discussion of SLA management for voice over IP in

the context of ETS. One of the key distinctions for ETS, as compared to publicly available services, is the emphasis on KQIs under abnormal (e.g., overload) conditions.

In order to address network availability and reliability requirements, the ETS examples found in [b-TMF GB917] and [b-TMF GB934] may be used, particularly the discussion of voice service aspects found in [b-TMF GB934]. Additional ETS-specific SLA management work, which could address development for data and video KQIs, is for further study.

7.16 ETS use of cloud infrastructure

[ITU-T Y.3501] provides general cloud computing requirements and capabilities. Annex A of this Recommendation contains the list of emergency telecommunications functional requirements and capabilities. Support for these requirements is needed when emergency telecommunications including ETS is offered by the cloud service provider (CSP) [ITU-T Y.3510].

The cloud computing infrastructure that is currently being defined may be used by service providers (e.g., NGN providers) to support public network services such as emergency telecommunications including ETS. If the cloud computing infrastructure is used to support emergency telecommunications including ETS, the network resources and core transport network requirements for priority treatment as specified in this Recommendation are applicable, and would need to be accommodated. For example, ETS provides priority telecommunications to the ETS authorized users in times of disaster and emergencies. In the context of cloud resource management, if the cloud infrastructure is used to support public network services, authorized ETS users should be able to obtain priority access (i.e., preferential treatment) to the cloud resources. In addition, the emergency telecommunications requirements as specified in this Recommendation apply across multiple layers of the cloud reference architecture defined in [ITU-T Y.3501] and [ITU-T Y.3510].

[ITU-T Y.3520] provides an overview of general concepts of end-to-end cloud computing resource management requirements. If cloud computing resources are used to support ETS, according to [ITU-T Y.3520] appropriate resource management functions will be needed to allow priority treatment in the use of cloud computing resources by authorized users.

Appendix IV of [ITU-T Y.3510] provides some guidance and details on ETS use of cloud infrastructure resources relevant to both network resources and core transport network requirements specified in this Recommendation.

Annex A

A possible distinction between essential and optional requirements

(This annex forms an integral part of this Recommendation.)

Emergency telecommunications functional requirements and capabilities	Description	Essential	Optional
Enhanced priority treatment	Emergency traffic needs assured capabilities regardless of the networks traversed.	X	
Secure networks	Networks should have protection against corruption of, or unauthorized access to, traffic and control (fraud), including expanded encryption techniques and user authentication, as appropriate.	X	
Location confidentiality	A limited number of high level leadership emergency telecommunication users may need to be able to use emergency telecommunications without risk of being located.		X
Restorability	Certain network functionalities should be capable of being reprovisioned, repaired, or restored to required levels on a priority basis.		X
Network connectivity	Networks supporting emergency telecommunications should provide international connectivity when possible, e.g., when [ITU-T E.106] and/or [ITU-T E.107] is applicable.	X	
Interoperability	Provide interconnection and Interoperability among all networks (evolving or existing).	X	
Mobility	The telecommunications infrastructure should support user and terminal mobility including re-deployable, or fully mobile telecommunications.	X	
Ubiquitous coverage	Public telecommunication infrastructure resources over large geographic areas should form the framework for ubiquitous coverage of emergency telecommunications.	X	
Survivability/endurability	Capabilities should be robust to support surviving users under a broad range of circumstances.	X	
Voice transmission	Circuit-switched and packet-switched networks should provide voice-band quality service for emergency telecommunications users.	X	
Video transmission	Circuit-switched and packet-switched networks should provide Quality of Service with low packet error rate and loss for emergency telecommunications users.	X	
Data transmission	Packet-switched networks should provide Quality of Service with low packet error rate for emergency telecommunications users.	X	

Emergency telecommunications functional requirements and capabilities	Description	Essential	Optional
Scaleable bandwidth	Authorized users should be able to select the capabilities of emergency telecommunications to support variable bandwidth requirements.		X
Reliability/availability	Telecommunications should perform consistently and precisely according to their design requirements and specifications, and should be usable with high confidence.	X	
Preferential treatment in congestion control mechanisms	Congestion control mechanisms should support reduced measures for emergency telecommunications traffic compared to normal traffic.		X

Appendix I

Information on possible sources of disasters

(This appendix does not form an integral part of this Recommendation.)

Two types of forces produce most natural disaster events. These are: extreme weather conditions (storms), and earthquakes. Both can dissipate variable amounts of energy and produce different damage over various geographic areas. The hurricane (sometimes referred to as a typhoon or cyclone) generally covers wide geographic areas and is the most devastating extreme weather storm condition on earth. The wind, rain, and secondary effects such as floods from this type of storm often cause widespread and lasting damage to properties and people. Although many aspects (such as intensity and paths) of storms are somewhat predictable and can provide precious warning times to people, damage to properties and land still occurs. In contrast to extreme weather conditions, earthquakes are largely unpredictable, but confined to smaller geographic areas. Nevertheless, powerful forces of nature are still unleashed and significant damage to properties and people often occur, especially in densely populated areas of the world.

Typically, natural disasters often set off additional clamorous events. For example, a hurricane may induce flash floods and mudslides. Hurricanes may cause rivers to overflow resulting in the death of livestock or damaged crops. People can be left without electricity or homes leaving them in need of food, clothing and shelter. Earthquakes continue to create damage after the initial quake through aftershocks. Sometimes earthquakes induce tidal waves that inflict additional damage to an already affected area. As seen in the recent past, some of these disasters may cascade and challenge the various measures planned to address them. An earthquake may set off effects in a nuclear facility, for example, and a chain of events that may not have been contemplated or considered when planning the response measures.

Some natural disasters are presented in Table I.1.

Table I.1 – Natural disasters

Avalanches
Drought
Earthquakes
Epidemics
Flash floods
Famine
Floods
Forest fires
Lightning
Hurricanes
Mudslides
Severe cold, snow, ice or heat
Tidal waves
Tornados
Tsunamis
Typhoons
Volcano eruptions
Wind storms

Disaster events that stem from human sources can also vary in energy, geographic distribution, duration, and damage potential.

Human caused disasters can rival those of nature. As with natural disasters, there may be additional ramifications stemming from the initial event. For example, a fire in a coal-mine can result in loss of life from burns or smoke inhalation. Such fires may trap people inside the coal-mine and lead to other explosions. A list of disasters caused by humans can be found in Table I.2.

Table I.2 – Man-made disasters

Arson
Chemical spills
Collapse of industrial or domestic structures
Explosions
Fires
Gas leaks
Nuclear explosions
Pipeline ruptures
Plane crashes/emergency landings
Poisoning
Radiation
Ships sinking/colliding
Stampedes
Subway collisions/derailments
Terrorism
Train collisions/derailments
Water-borne accidents

Bibliography

[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*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014