INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Y.1271

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(10/2004)

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

ITU-T Recommendation 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
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
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

ITU-T Recommendation 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.

Source

ITU-T Recommendation Y.1271 was prepared by ITU-T Study Group 13 (2001-2004) and approved on 14 October 2004 by the World Telecommunication Standardization Assembly (Florianópolis, 2004).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

		Page
1	Introduction	1
2	Scope	1
3	References	1
4	Definitions	1
5	Abbreviations	2
6	Security	2
7	Consideration	3
7.1	The nature of emergency situations	3
7.2	Emergency response	3
7.3	Assured telecommunications	3
8	Emergency telecommunications requirements and capabilities	4
8.1	Enhanced priority treatment	4
8.2	Secure networks	6
8.3	Location confidentiality	6
8.4	Restorability	7
8.5	Network connectivity	7
8.6	Interoperability	7
8.7	Mobility	8
8.8	Ubiquitous coverage	8
8.9	Survivability/endurability	8
8.10	Voice transmission	8
8.11	Scaleable bandwidth	8
8.12	Reliability/availability	9
Annex A – A possible distinction between essential and optional requirements		10
Appendix I – Information on possible sources of disasters		11

ITU-T Recommendation Y.1271

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

1 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. 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 that is evolving from a basic circuit-switched to packet-switched networks with a variety of telecommunication capabilities.

2 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 should 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 Rec. E.106 if needed.

3 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 Recommendation E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

4 Definitions

This Recommendation defines the following terms:

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

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

4.3 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.

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

4.5 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.

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

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

4.8 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.

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

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

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

4.12 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.

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

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

4.15 preferential: A capability offering advantage over regular capabilities.

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

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

5 Abbreviations

This Recommendation uses the following abbreviations:

QoS Quality of Service

SLA Service Level Agreement

6 Security

Due to the nature of this Recommendation, security is addressed in general. However, special attention should be given to clause 8 where several requirements may have strong security implications, such as network integrity (8.2), secrecy aspects of selected users (8.3), network restorability (8.4), interoperability (8.6), survivability/endurability (8.9) and reliability/availability (8.12). Other ITU-T Recommendations may complete this Recommendation with regard to security aspects.

7 Consideration

7.1 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.

7.2 Emergency response

All types of disasters, whether attributed to natural or human sources, can strike anywhere and anytime. 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.

7.3 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 are offered, users of the service should be authorized. 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.

Circuit-switched networks respond to overload situations by denying call attempt when resources are saturated. One option is to pre-empt other callers when authorized emergency communication workers need to communicate. However, some types of networks respond to an additional load by degrading performance of 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.

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.

8 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/Y.1271 – Emergency telecommunications functional requirements and capabilities

Enhanced priority treatment
Secure networks
Location Confidentiality
Restorability
Network connectivity
Interoperability
Mobility
Ubiquitous coverage
Survivability/endurability
Voice transmission
Scaleable bandwidth
Reliability/availability

8.1 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 (SP) 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 communications.

8.1.1 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.

8.1.2 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.

8.1.3 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.

8.1.4 Optional pre-emption of non-emergency traffic

While the concept of pre-emption typically applies to circuit-switched communications, its application in connectionless network services, if determined viable, needs to be studied and defined. Pre-emption of non-emergency traffic to free bandwidth and resources for emergency traffic is an optional requirement; the basic emergency telecommunication provisions do not include the concept of pre-emption.

---

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

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

The QoS for different modes of service for the emergency telecommunication 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. An ordinary telecommunications may be degraded or released.

8.2 Secure networks

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

8.2.1 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.

8.2.2 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.

8.3 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.

8.4 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.

8.5 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 Rec. E.106 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.

8.6 Interoperability

Evolving networks will produce a number of issues, one of which is to ensure orderly and transparent continuance of the basic ITU-T Rec. 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 preferential treatment methods over heterogeneous networks needs to be addressed.

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).

8.7 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.

8.8 Ubiquitous coverage

Ubiquitous telecommunications resources that provide support to services of the general population may provide the basis for readily available capabilities for emergency communications. 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 communications.

8.9 Survivability/endurability

Key network infrastructure supporting emergency communications 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.

8.10 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 need to provide voice transmission quality service for emergency telecommunications users.

8.11 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 scaleable 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.

8.12 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.

Telecommunications should perform consistently and precisely according to their design requirements and specifications, and should be usable with high confidence.

Annex A

A possible distinction between essential and optional requirements

Emergency communications 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 Rec. E.106 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 need to provide voiceband quality service for emergency telecommunications users.	X	
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	

Appendix I

Information on possible sources of disasters

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. Some natural disasters are presented below.

Table I.1/Y.1271 – 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 human caused disasters can be found below.

Table I.2/Y.1271 – Human-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 born accidents

In addition to the above disaster examples, some example scenarios for emergency telecommunications are listed below.

- Multiple emergency organization locations with access links into the same network where the provider offers QoS. Note that the particular provider, access link bandwidth, and local configurations can be determined in advance of the emergency.
- Emergency Worker accesses an Internet via arbitrary connection (e.g., Internet Cafe). Note that the Internet Service Provider granting connectivity to the Internet cannot be determined in advance.
- A predetermined network is connected to a privately managed packet network over a predetermined constrained bandwidth connection (e.g., Government First Responder Organization connecting to a packet network using a low-bandwidth satellite link).
- A database available on the public Internet supporting emergency services/recovery (e.g., Japan's IAA).
- Circuit-switched and packet-switched telephony interworking scenarios (IP origination to circuit network, circuit network to packet network to circuit network, circuit network to packet network, end-to-end packet network).

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	Telephone transmission quality, telephone installations, local line networks
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, 2005