International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2205

(09/2008)

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

Next Generation Networks – Service aspects: Service capabilities and service architecture

Next Generation Networks – Emergency telecommunications – Technical considerations

Recommendation ITU-T Y.2205

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.

Recommendation ITU-T Y.2205

Next Generation Networks – Emergency telecommunications – Technical considerations

Summary

Recommendation ITU-T Y.2205 specifies technical considerations that may be applied within the next generation network (NGN) to enable emergency telecommunications (ET). In addition, this Recommendation also outlines the underlying technical principles involved in supporting emergency telecommunications.

Source

Recommendation ITU-T Y.2205 was approved on 12 September 2008 by ITU-T Study Group 13 (2005-2008) under the WTSA Resolution 1 procedure.

Keywords

Architecture, early warning (EW), emergency telecommunications service (ETS), emergency telecommunications, NGN, priority telecommunications, QoS, telecommunications for disaster relief (TDR).

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/.

CONTENTS

Introduction

[ITU-T Y.1271] provides the network requirements and capabilities for emergency telecommunications (ET). The realization of priority telecommunications based upon those requirements, as exemplified by authorities coordinating disaster relief using public networks, may result in the creation of new mechanisms and interworking/reuse of existing mechanisms. Emergency telecommunications should be given preferential treatment over regular public network services. Prioritized telecommunications used in emergency situations are not new; circuit-switched networks have supported such systems for years, primarily for voice calls (e.g., [ITU-T E.106]). However, the technical methods used to support these underlying requirements for emergency telecommunications in the NGN environment are evolving. Traditional circuit switched priority methods do not necessarily apply in NGN due to inherent differences in circuit-switched versus packet-switched telecommunication.

[ITU-T Y.1271] outlines the requirements and capabilities in general and abstract terms. [ITU-T Y.1271] is technology neutral.

Since NGN is based on packet-switched technology, which is fundamentally different from circuit-switched technology, there is a need to consider the technical issues and potential solutions that could be used to effect the realization of emergency telecommunications capabilities in NGN.

This Recommendation specifies technical considerations that may be applied within NGN to enable emergency telecommunications and the underlying principles involved.

Recommendation ITU-T Y.2205

Next Generation Networks – Emergency telecommunications – Technical considerations

1 Scope

This Recommendation specifies technical considerations that may be applied within the next generation network (NGN) to enable emergency telecommunications (ET). In addition, this Recommendation also outlines the underlying technical principles involved in supporting ET. It specifies requirements and capabilities for ET beyond the ones specified in [ITU-T Y.2201] in the context of NGN (as defined in [ITU-T Y.2001] and further outlined in [ITU-T Y.2011]).

Emergency telecommunications (including support of some aspects of early warning (see Figure 1)) include:

- individual-to-authority emergency telecommunications, e.g., calls to emergency service providers;
- authority-to-authority emergency telecommunications;
- authority-to-individual emergency telecommunications, e.g., community notification services.

Appendix I provides additional information for the above listed ET categories.

Some requirements and capabilities for early warning are also specified. Individual-to-authority emergency telecommunications capabilities are not addressed and are outside the scope of this Recommendation.

Some of the technical means described herein could also be used for individual-to-authority or individual-to-individual emergency telecommunications; however, these categories are not addressed in this Recommendation.

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 H.248.1] Recommendation ITU-T H.248.1 (2005), *Gateway control protocol: Version 3.*

[ITU-T H.323] Recommendation ITU-T H.323 (2006), *Packet-based multimedia communications systems.*

[ITU-T H.460.4] Recommendation ITU-T H.460.4 (2007), *Call priority designation and country/international network of call origination identification for H.323 priority calls.*

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

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications.*

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

[ITU-T Y.110] Recommendation ITU-T Y.110 (1998), *Global Information Infrastructure principles and framework architecture.*

[ITU-T Y.1271] Recommendation ITU-T Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks.*

[ITU-T Y.1541] Recommendation ITU-T Y.1541 (2006), *Network performance objectives for IP-based services.*

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

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1.*

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks.*

[ITU-T Y.2171] Recommendation ITU-T Y.2171 (2006), *Admission control priority levels in Next Generation Networks.*

[ITU-T Y.2172] Recommendation ITU-T Y.2172 (2007), *Service restoration priority levels in Next Generation Networks.*

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements.*

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification.* <http://www.ietf.org/rfc/rfc2205.txt?number=2205>

[IETF RFC 3246] IETF RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behavior).* <http://www.ietf.org/rfc/rfc3246.txt?number=3246>

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.* <http://www.ietf.org/rfc/rfc3261.txt?number=3261>

[IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).* <http://www.ietf.org/rfc/rfc3312.txt?number=3312>

[IETF RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP).* <http://www.ietf.org/rfc/rfc4412.txt?number=4412>

[IETF RFC 4542] IETF RFC 4542 (2006), *Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite.* <http://www.ietf.org/rfc/rfc4542.txt?number=4542>

[IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes.* <http://www.ietf.org/rfc/rfc4594.txt?number=4594>

3 Definitions

This Recommendation uses definitions from: [ITU-T Y.1271], [ITU-T Y.2001], [ITU-T Y.2011] and [ITU-T Y.2201].

3.1 emergency telecommunications (ET): ET means any emergency related service that requires special handling from the NGN relative to other services. This includes government authorized emergency services and public safety services.

3.2 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.

3.3 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.

3.4 telecommunications for disaster relief (TDR): TDR is an international and national telecommunications capability for purposes of disaster relief. It can make use of international permanent, shared network facilities already in place and operational, temporary network facilities that are provisioned specifically for TDR, or a suitable combination of the two.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ASN.1 Abstract Syntax Notation One

CAC Call Admission Control

CAP Common Alerting Protocol

DoS Denial of Service

DSCP Differentiated Services Code Point

EAS Emergency Alert System

EF Expedited Forwarding

ENI ETS National Implementation

ET Emergency Telecommunications

ETS Emergency Telecommunications Service

EW Early Warning

IEPS International Emergency Preference Scheme

IP Internet Protocol

ISDN Integrated Services Digital Network

MMPS Multimedia Priority Service

NGN Next Generation Network

NOAA National Oceanic and Atmospheric Administration

PHB Per Hop Behaviour

PIN Personal Identification Number

PLMN	Public Land Mobile Network
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RACF	Resource and Admission Control Function
RPH	Resource Priority Header
RSVP	Resource ReSerVation Protocol
QoS	Quality of Service
SAME	Specific Area Message Encoding
SCF	Service Control Function
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SS7	Signalling System No. 7
TCP	Transmission Control Protocol
TDR	Telecommunications for Disaster Relief
UDP	User Datagram Protocol
UN/ISDR	United Nations International Strategy for Disaster Reduction
VoIP	Voice over IP
W-CDMA	Wideband Code Division Multiple Access
WPS	Wireless Priority Service
xDSL	Any variant of Digital Subscriber Line
XML	eXtensible Markup Language
XSD	XML Schema Definition

5 Emergency telecommunications (ET) and early warning description

5.1 General

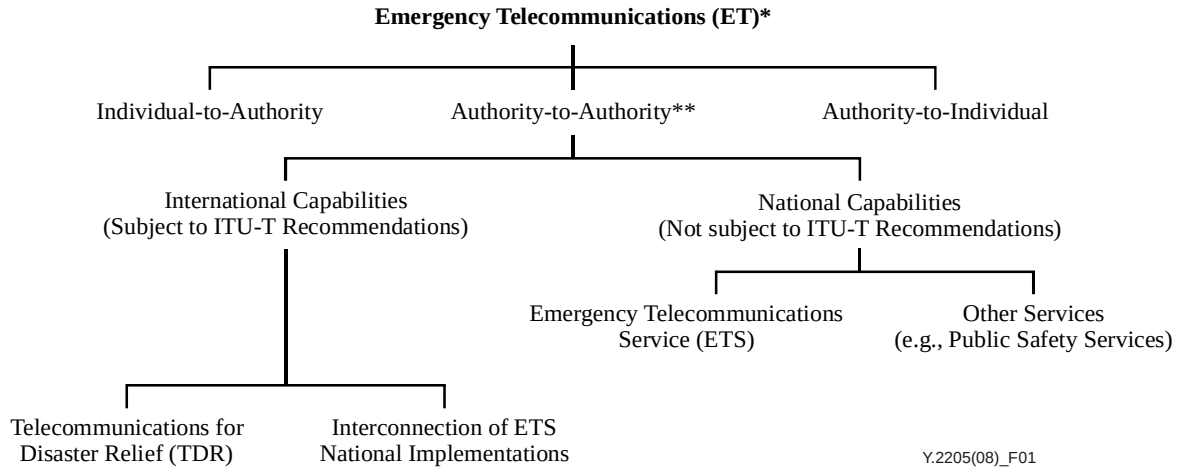
The following terms are used in this Recommendation:

- emergency telecommunications ET
- emergency telecommunications service ETS
- telecommunications for disaster relief TDR
- early warning EW

It is essential that the different uses of these terms are agreed and understood. To that end, the following terms are used in the following manner:

- ET The umbrella term for any emergency related service that requires special handling from the NGN relative to other services.
- ETS The term is used as defined in [ITU-T E.107].
- TDR The generic term for a telecommunications capability used for the purposes of disaster relief.
- EW The generic term for all types of early warning systems/capabilities/services.

This arrangement forms a tree with ET at the root for all activities. The use of terms and their inter-relationships is shown in Figure 1 below.



* Including some aspects of Early Warning
** May also apply to authority-to-individual telecommunications

Figure 1 – Terminological relationship framework for emergency telecommunications

5.2 Emergency telecommunications

Emergency telecommunications (ET) means any emergency related service that requires special handling from the NGN relative to other services. This includes government authorized emergency services and public safety services. The following are specific example services under the umbrella of emergency telecommunications:

1) *Telecommunications for disaster relief (TDR)*

   TDR is an international and national telecommunications capability for the purpose of disaster relief. It can make use of international permanent, shared network facilities already in place and operational, temporary network facilities that are provisioned specifically for TDR, or a suitable combination of the two.

2) *Emergency telecommunications service (ETS)*

   ETS is a national service, providing priority telecommunications to ETS authorized users in times of disaster and emergencies. The description of ETS is specified in [ITU-T E.107]. [ITU-T E.107] provides guidance that will enable telecommunications between one ETS national implementation (ENI) and other ENI(s) (authority-to-authority).

3) *National/Regional/Local emergency and public safety services*

   Other examples of ET are national/regional/local emergency and public safety services. These are specialized services for national/regional/local emergencies and public safety. These emergency services are national/regional/local specific and are subject to national/regional standardization.

5.3 Early warning

The United Nations International Strategy for Disaster Reduction (UN/ISDR) in a September 2006 report [b-UN Global Survey] to the United Nations Secretary-General on a "Global Survey of Early Warning Systems" which defines early warning as "the provision of timely and effective information, through identified institutions, that allows individuals exposed to a hazard to take action to avoid or reduce their risk and prepare for effective response". This UN report provides an

assessment of capabilities, gaps, and opportunities towards building a comprehensive global early warning system for all natural hazards.

6 General considerations for emergency telecommunications and early warning

Prior to the development of [ITU-T Y.1271], the requirements for emergency telecommunications capabilities primarily related to circuit-switched networks such as the public switched telephone network (PSTN).

These requirements were based on and took advantage of certain characteristics of circuit-switched networks. For example:

- admission control utilizing a tight coupling between signalling and media resources;
- all media traffic requiring uniform bandwidth delivered at a constant bit rate;
- per flow reserved bandwidth;
- separation of control and data traffic.

These characteristics are not necessarily found in current best-effort packet-switched networks where:

- packet-switched networks tend to rely on sharing resources and using queues to help compensate for bursty traffic – the combination generally realized as best-effort service;
- admission control may be difficult – many applications do not signal their bandwidth requirements, and there is a decoupling of signalling and media;
- applications/services have variable bandwidth requirements and may send data using dynamically adjusted rates;
- different packet flows share statistically multiplexed bandwidth;
- resource control and data traffic may share the same resources in the network.

In packet-switched NGN, packets may still contend for available bandwidth, unless special measures are applied. At a pure transport level, packets cannot easily be refused or flow-controlled. Additionally, traffic engineering of a packet-based network is significantly different from a circuit-switched network with regard to standard and universally accepted approaches. A given "flow" of packets can be affected by other flows of packets using a shared resource, unless special measures available in an NGN are utilized appropriately. On the other hand, the separation between service and transport in an NGN may be advantageous for provisioning of more flexible and diverse emergency capabilities.

These conditions mean that the provisioning of emergency telecommunication capabilities is not entirely straightforward, obvious or simple, nor can simple transposition from the circuit-switched world be affected. Other detailed differences between circuit-switched and packet-switched networks, and between different packet technologies, will affect the provisioning and fulfilment of the various requirements specified in [ITU-T Y.1271].

Thus, the intent of this Recommendation is to indicate what features and mechanisms of an NGN may be used to facilitate the requirements of emergency telecommunications and some aspects of early warning.

7 General functional requirements and capabilities

Functional requirements and capabilities include those specified in [ITU-T Y.1271] and [ITU-T Y.2201] for release 1 NGN, and in addition those detected from the UN Global Survey on Early Warning Systems with relevance to NGN development [b-UN Global Survey].

7.1 Emergency telecommunications

Table 1 lists the emergency telecommunications functional requirements and capabilities.

Table 1 – Emergency telecommunications functional requirements and capabilities list

Emergency telecommunications functional requirements and capabilities
Enhanced priority treatment
Secure networks
Location confidentiality
Restorability
Network connectivity
Interoperability
Mobility
Ubiquitous coverage
Survivability/endurability
Real-time transmission to support: voice/real-time text and video/imagery (where bandwidth is available)
Non-real-time transmission to support: messages/non-real-time streams (audio/video)
Scalable bandwidth
Reliability/availability

The goal is to provide high confidence and probability that critical telecommunications will be available to perform reliably for authorized users, such as those involved in emergency telecommunications. [ITU-T Y.1271] provides "Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks".

With respect to video and imagery, bandwidth (e.g., a form of resource) availability should be taken into consideration.

7.2 Early warning

Some objectives for early warning systems in the context of the NGN are to*:*

- have continuously operating capabilities and be operational, robust, available every minute of every day;
- provide warning messages only to those possibly affected by an impending disaster;
- provide the needed telecommunication capabilities to transmit real-time (e.g., seismic and sea-level data information);
- be based on internationally agreed standards;
- ensure that only authorized messages are sent;
- prevent untargeted and unnecessary messages (e.g., messages sent to the wrong people and/or messages that do not contain useful viable information).

Additional objectives may include capabilities to support the filtering of messages so that these reach a select:

- group of users;
- regions, etc.

(e.g., a form of "cell broadcasting")

8 Mechanisms and capabilities supporting emergency telecommunications in NGN

8.1 General

The separation of service/application control from transport, which allows both application services and transport services to be offered separately and to evolve independently, is a key characteristic of NGN. This separation takes the form of two distinct blocks or strata of functionality. The transport functions reside in the transport stratum and the service control functions related to applications, such as telephony, reside in the service stratum. In general, each stratum will have its own set of roles, players and administrative domains (see [ITU-T Y.110]). The roles involved in service(s) provisioning are independent from those involved in transport connectivity provisioning. Each stratum can be treated separately from a technical point of view. The resource and admission control functions (RACF) is the arbitrator between these strata for QoS-related reservation (and negotiation) in the NGN architecture. [ITU-T Y.2111] specifies the functional architecture and requirements for the resource and admission control functions in next generation networks, which may involve a variety of access and core transport technologies and multiple domains. The RACF QoS-related decisions are based upon SLAs, service priority, user profiles, network operator policy rules and resource availability for both access and core networks. Emergency telecommunications users are required to be identified and given priority for admission control by the RACF once authenticated and authorized.

If emergency telecommunications traffic is to be distinguished from normal traffic within the NGN, then appropriate distinguishing labels, also known as markers, are required to be available. The term (traffic) marking is used in this context.

In the edge-to-edge (i.e., access and core network segments) multi-layered (i.e., transport and service strata) NGN protocol architecture, labels may exist in various forms at the different protocol layers both vertically (i.e., interactions between different protocol layers) and horizontally (i.e., interactions between communicating network elements). Labels can be carried in signalling packets, and/or included within the header of a data packet to identify and mark emergency telecommunication calls/sessions. The labels used to identify and mark emergency telecommunications calls/sessions and/or traffic are protocol specific. To achieve specialized (e.g., priority/preferential) treatment end-to-end for all aspects of the emergency telecommunication call/session (i.e., call/session control, bearer traffic and management), appropriate mapping and interworking between the labels used in the different protocols are required. For example, the SIP resource priority header information used in the control layer to identify priority call/session could be mapped to the appropriate diff-serv code points (DSCPs) to mark the emergency telecommunications traffic in the IP network layer. Similarly, the diff-serv code points (DSCPs) at layer 3 could be mapped to the specific VLANs or Ethernet priority parameters at layer 2 in the transport protocol. SIP is specified in [IETF RFC 3261] and its updates [b-IETF RFC 3265], [b-IETF RFC 3853], [b-IETF RFC 4320], [b-IETF RFC 4916], [b-IETF RFC 4032], and [b-IETF RFC 5027].

In the service stratum, services tend to use a specific and designated set of protocols. Thus, the techniques that can be leveraged for specific emergency telecommunications services will vary according to the services under consideration and the capabilities of the particular service-related protocol(s) in question.

In the transport stratum, the Internet Protocol (IP) may be used. The exact composition of the underlying IP protocol stack is likely to vary from one provider to another.

Furthermore, the protocols used in local (last-mile) access infrastructures may be different from those used in core infrastructures. Local access infrastructures could be wired (i.e., fixed access), wireless, or a combination of these two technologies.

Thus, a given end-to-end path for an emergency telecommunication call/session can traverse a wide range of transport technologies.

Later clauses will outline the various features and/or capabilities of particular technologies that can be leveraged to facilitate the requirements of emergency telecommunications.

Since the transport stratum may use the IP (and a number of related protocols), such as TCP or UDP defined by the IETF, it is prudent to utilize applicable IETF-defined capabilities in respect of its usage for support of emergency telecommunications, as applicable. These will be discussed in later clauses.

It is important to make a distinction between the specifications (RFCs) developed by the IETF, and their deployment in the Internet, and/or an NGN context. In both cases, the actual specifications used will depend on what the particular provider concerned has deployed. However, since the Internet is outside the scope of ITU-T, no assumptions can be made about the quality of service or capabilities of Internet-based paths, as explained in [b-IETF RFC 4190][1]. On the other hand, more stringent requirements for international emergency telecommunications in IP-based NGNs are within the scope of ITU-T and may be proposed in ITU-T Recommendations for use by NGN providers.

[IETF RFC 4542] describes possible solutions for the "Internet Emergency Preference Service". Many of the concepts outlined therein apply to ETS in the context of NGN.

In a NGN where the service and transport stratum are independent, it follows that the following factors influence the success of an emergency telecommunication:

i) identification and marking of the emergency telecommunication traffic;

ii) admission control policy;

iii) bandwidth allocation policy;

iv) authentication and authorization of bona-fide emergency telecommunications users.

8.1.1 Priority treatment

In general, priority treatment is the key to providing emergency telecommunications, which by definition have to be considered more important than ordinary telecommunication services. When ordinary services consume the vast majority of finite network resources, emergency telecommunications are forced to compete for these same finite resources, and can be adversely affected. Therefore, some means of giving priority treatment for emergency services over ordinary telecommunication services should be devised. Primarily, this means:

a) Recognizing the authorized emergency telecommunications users;

b) Granting the authorized emergency telecommunications users service priority.

---

[1] [b-IETF RFC 4190] states:

"A constant fixture in the evolution of the Internet has been the support of Best Effort as the default service model", and:

"inter-domain ETS communications should not rely on ubiquitous or even widespread support along the path between the end points."

In the layered NGN architecture as defined in [ITU-T Y.2012], the priority indicator sent from the service control function (SCF) to the resource and admission control function (RACF) should be capable of indicating priority levels associated with the users to allow different policies to be implemented and differentiation between multiple types of priority applications. For example, hospital personnel might be provided a user priority level below that of critical emergency relief coordinators.

8.1.2 Identification, authentication and authorization, and access control

It is necessary to prevent unauthorized access to services and resources for emergency telecommunications, such as by intruders masquerading as authorized users. Therefore, mechanisms and capabilities to authenticate and authorize access of emergency telecommunications users, devices or user and device combinations as applicable based on policy for specific service (e.g., ETS and TDR) are required to be supported.

It is necessary to identify emergency telecommunications call/session requests (e.g., by specialized dialling, input, user or subscription profiles). NGN providers should expedite the authentication of authorized emergency telecommunications users. Specific mechanisms and methods are required to be used for authentication and authorization based on policy for specific emergency telecommunications (e.g., use of personal identification number (PIN), and user and subscription profiles). Once the user, user device or user and device combination is authenticated and authorized based on the applicable policy, the emergency telecommunications call/session is required to be marked and indicated in the forward direction to subsequent networks. Also once authenticated and authorized, priority is required to be given to all aspects of the emergency telecommunications call/session, the signalling/control, the bearer traffic, and any applicable management.

Authentication and authorization consideration is also required to be given to the handing off and receiving of emergency telecommunications calls/session between NGN providers, taking into account a multi-provider environment and separation of service control and transport. Authentication and authorization of NGN providers for handing off and receiving emergency telecommunications calls/session and traffic should be based on SLAs and applicable policy.

8.1.3 Admission control considerations for higher probability of admission

One of the functions of the resource and admission control function (RACF) is to support QoS control to include resource admission and resource reservation, if desired, by the service provider. As such, during times of high service demand from users, some service requests may need to be denied. If these denials do not occur, then the NGN may not fully guarantee service quality in emergency cases. The RACF QoS-related processes involve authorization based on user profiles, SLAs, operator specific policy rules, service priority, and resource availability within access and core transport. This Recommendation postulates that RACF should have the capability to prioritize service requests using service priority. (A network that simply denied authorized requests due to momentary congestion would lead to poor customer service if customers were repeatedly forced to re-submit requests.) Therefore, this Recommendation asserts that service priority is a primary factor to be considered by the scheduling method for the resource allocation queue/general admission decision. Mechanisms to enable this functionality are discussed below.

The high-level requirements of the RACF are to operate on authorized requests for QoS using user profiles and priority. One specific requirement is for admission control to make use of the service priority information for priority handling. There are various methods that can be used for resource-based admission control service priority.

One possible method is that a higher admission threshold be provided for emergency telecommunications traffic, thus allowing some additional admission for priority requests when regular requests are being denied. In effect, this method temporarily increases utilization of network resources. However, because of the large amount of NGN resources and the fact that in any appreciable time interval, some resources will naturally become available (e.g., as other sessions

complete) the system will be restored to its intended operational day-to-day traffic capability. Furthermore, assuming that the amount of priority traffic is relatively small and networks seldom, if ever, operate at full 100 percent capacity, it becomes clear that the higher threshold of the admission decision for priority traffic should not pose any danger to the overall network health or QoS of other traffic.

There are reservation-based admission control systems that allow a service request only when the request for required bandwidth is successful. In this case, the method of servicing the scheduling mechanisms should consider service priority as a primary consideration.

Finally, other mechanisms to bypass admission control mechanisms are also possible (e.g., priority traffic bypassing RACF). The use of the resource reservation protocol mechanism as described in [b-IETF RFC RSVP] is an example of such a mechanism.

8.1.3.1 Call admission control (CAC)

CAC is a set of actions/policies taken by the network at call/session setup phase in order to accept or reject a service based on requested performance and priority criteria, and the availability of necessary resources.

In a traditional PSTN/ISDN, call admission control simply means whether a circuit is granted or not based on the authorization. Furthermore, allocation of a circuit by definition implies the availability of a path with the required bandwidth. Due to the availability of network state information regarding the status of individual circuits (voice-band channels), a PSTN/ISDN network can:

a) divert emergency calls to paths specifically reserved for emergency traffic (if available);

b) wait for a circuit to be available (trunk queuing).

Since no discrete paths or circuit state information exist in IP-based networks, authentication and authorization at the ingress to the network alone cannot ensure availability of an end-to-end path or sufficient end-to-end bandwidth for a given call/session. In an IP-based network, an ingress network element has no or little knowledge of prevailing network conditions outside its domain. Therefore, CAC at an ingress network element is insufficient to ensure availability of an end-to-end path unless augmented by additional mechanisms.

A further implication is that an egress network element has no control over or knowledge of the remote ingress network element that may be attempting to establish a call/session to it. However, in a PSTN/ISDN an egress network element is able to control a potential ingress network element, attempting to establish a call/session, via the associated signalling mechanisms.

[ITU-T Y.2171] specifies admission control priority for telecommunications services seeking entry into a network particularly during emergency conditions when network resources may be depleted. In particular, it recommends three levels for admission control priority for services seeking entry into NGN. Priority level 1 (highest) is recommended for emergency telecommunications (including ETS) over NGN. Traffic with this priority level receives the highest priority for admission to the NGN.

8.2 Service stratum

8.2.1 General

Countries have, or are developing, ETS to allow priority treatment for authorized traffic to support emergency and disaster relief operations within their national boundaries. However, there could be a crisis situation where it is important for an ETS user in one country to communicate with available users in another country. In this case, it is important for an ETS call/session originated in one country to receive end-to-end priority treatment, i.e., priority treatment in the originating country and the destination country. This may require interconnection of two ETS national

implementations via an international network that either provides priority treatment capabilities, or convey the priority transparently between both countries.

The following clauses outline a number of protocol mechanisms used to signal and obtain priority treatment at the service control level in the context of a packet-based NGN. Specific applicability of these protocol mechanisms to ETS are also highlighted. These protocol capabilities are needed for international applications in the context of communications between national ETS implementations via the international network (e.g., interconnection of two ETS national implementations).

8.2.2 SIP resource priority

[IETF RFC 4412] adds two header fields to SIP, namely the Resource-Priority and the Accept-Resource-Priority fields, and specifies the procedures for their usage. The 'Resource-Priority' header field may be used by SIP user agents, including public switched telephone network (PSTN) gateways and terminals, and SIP proxy servers to influence their treatment of SIP requests.

To provide equivalence to some existing systems, priority appropriate to several different "standardized" systems can be accommodated by identifying the "namespace" appropriate to the particular system and the number of priority levels within that system. The following namespaces and the associated number of priority levels are identified in [IETF RFC 4412] for use in ETS.

Namespace	Levels
ets	5
wps	5

All ETS calls/sessions in IP environments are designated with an "ets" namespace with five priority levels that convey levels of importance in the application layer (within SIP elements). Incoming ETS calls/sessions are assigned the "ets" designation in the 'Resource-Priority' header. ETS calls/sessions are recognized by the presence of the "ets" namespace 'Resource-Priority' header value in the SIP message and accorded the "High" priority for resource reservation/assignment such that preferential treatment can be enacted in the transport layer. A similar namespace designation of "wps" accompanied by five priority levels is available for call/session allocations where resources are limited or congested, such as in radio access for wireless networks.

8.2.3 IEPS

[ITU-T E.106] describes the functional requirements, features, access and the operational management of the IEPS. IEPS allows interoperability of different national implementations of priority/preference schemes, thereby providing end-to-end preferential treatment to authorized narrow-band voice and data calls.

The scope of [ITU-T E.106] is framed in the context of the PSTN, ISDN or PLMN. The IEPS provides priority treatment for international telephony service for authorized users over connection-oriented telecommunications networks. Therefore, based on bilateral/multilateral agreement between countries/administrations, IEPS could be used in such a scenario for interconnection of ETS national implementations.

8.2.4 H.323 system control protocols

This clause outlines protocols used in the H.323 system in support of priority telecommunications.

[ITU-T H.460.4] specifies the call priority designation and country/international network of call origination identification for H.323 priority calls. The H.460.4 call priority designation parameter supports both the priority call indicator and five priority levels.

[ITU-T H.248.1] defines the protocols used between elements of a physically decomposed multimedia gateway, used in accordance with the architecture as specified in [ITU-T H.323]. For government authorized emergency services (e.g., ETS), [ITU-T H.248.1] defines the IEPS call indicator and priority indicator. The IEPS call indicator carries the priority indication between the

controller and gateway functions. The Priority indicator carries the priority levels between the controller and gateway functions and the H.248 Priority indicator supports 16 levels of priority. For public safety services, [ITU-T H.248.1] defines the emergency indicator for carrying the priority indication between the controller and gateway functions.

8.3 Transport stratum

8.3.1 General

The need for special arrangements (e.g., SLA) to handle ET in a properly engineered and dimensioned NGN is based on an assumption that the network resources are inadequate for the amount of traffic being offered to the network, and that under such conditions emergency telecommunications traffic could be rejected or significantly delayed and/or disrupted beyond the point of being usable, or even be discarded. When the amount of traffic being received with a statistically engineered, or best-effort, service model exceeds the capacity of a given receiving network element (e.g., an IP router) and/or the outgoing capacity available to the given element, the only recourse open to this network element is to discard the excess traffic. This means that emergency traffic would be discarded along with non-emergency traffic unless special preferential measures are enabled.

The technique of over-provisioning is sometimes advocated as a solution. However, over-provisioning may not be possible or practical in many cases, and more importantly, some kinds of emergencies may result from deliberate or accidental destruction/degradation of parts of the network, and thus eliminate any over-provisioned paths or elements that might normally have been available. Thus, the over-provisioning has negative impacts. If an NGN is to be capable of handling all kinds of emergencies under adverse circumstances, the availability of specific means to provide preferential treatment of emergency telecommunications traffic will be necessary.

The following clauses outline a number of mechanisms used to obtain priority treatment at the transport level in the context of a packet-based NGN.

8.3.2 Bandwidth control using RSVP

One possible feature of an IP-based network that is able to provide some (rough) equivalence to a circuit-based bandwidth allocation would be an IP-based mechanism for bandwidth allocation and reservation. This exists as a procedure defined by the IETF in its resource reservation protocol (RSVP) specified in [IETF RFC 2205] and its updates [b-IETF RFC 2750], [b-IETF RFC 3936], and [b-IETF RFC 4495].

The resource control parameterization necessary for session initiation protocol (SIP) in the service stratum to be used in conjunction with RSVP (in the transport stratum) is specified in [IETF RFC 3312]. This permits RSVP signalling to be used before, during and/or interwoven with the SIP signalling procedures. Some examples of this are given in Appendix A of [IETF RFC 4542]. However, [IETF RFC 4542] uses the pre-emption technique.

[b-IETF RFC RSVP] specifies RSVP extensions that can be used to support an admission priority capability at the network layer. It specifies new RSVP extensions to increase the probability of call completion without pre-emption. Engineered capacity techniques in the form of bandwidth allocation models are used to satisfy the "admission priority" required by an RSVP capable emergency telecommunications network. In particular, this document specifies two new RSVP Policy Elements allowing the admission priority to be conveyed inside RSVP signalling messages so that RSVP nodes are able to enforce selective bandwidth admission control decisions based on the call admission priority.

8.3.3 Queuing control using differentiated services

[IETF RFC 4594] outlines a recommended mapping between service classes and differentiated services code points (DSCP). Figure 3 of [IETF RFC 4594] includes a mapping table which

allocates the expedited forwarding class to telephony applications. This allows IP packets to contain a DSCP value allocated to the expedited forwarding class.

Furthermore, [ITU-T Y.1541] also recommended that voice traffic be marked (labelled) in the IP packets with the DSCP corresponding to EF. Network elements (routers) in the transport stratum receiving packets marked EF will assure timely delivery of time-critical traffic relative to non-time-critical traffic using the expedited forwarding behaviour defined for the EF code point and specified in [IETF RFC 3246].

However, the EF code is used for normal telephony traffic. Consequently, there may still be a need to somehow differentiate between emergency telephony traffic and non-emergency telephony traffic, see next clause.

8.3.4 EF DSCP for capacity-admitted traffic

[b-IETF RFC DSCP] allocates an EF DSCP for capacity-admitted traffic. This would permit real-time traffic conforming to the expedited forwarding per hop behaviour using a CAC procedure involving authentication, authorization, and capacity admission (see 8.3.1 and 8.3.2 above) as opposed to a class of real-time traffic conforming to the expedited forwarding per hop behaviour that has not been subject to capacity admission.

It has been proposed that the requested code point should be referred to as EF-ADMIT and assigned an appropriate value.

8.4 NGN access

8.4.1 General

There are multiple technology-dependent methods for NGN access. According to [ITU-T Y.2012] the access network includes access-technology dependent functions, e.g., for W-CDMA technology and xDSL access. Depending on the technology used for accessing NGN services, the access network includes functions related to:

1) Cable access
2) xDSL access
3) Wireless access (e.g., IEEE 802.11 and 802.16 technologies, and 3G RAN access);
4) Optical access.

To support emergency telecommunications, special arrangements are also needed in the NGN access segment. The need for special arrangements is based on the assumption that in the same way that the core network resources are limited, access resources are also limited. Therefore, depending on the amount of traffic being offered to the access network segment, emergency telecommunications traffic could be impacted (e.g., rejected or significantly delayed and/or disrupted beyond the point of being usable, or even be discarded).

Therefore, if the NGN is to be capable of handling all kinds of emergencies under adverse circumstances, the availability of specific means to provide preferential treatment of emergency telecommunications traffic needs to be supported in the NGN access segment. This includes, but is not limited to mechanisms and capabilities for:

- recognizing emergency telecommunications traffic;
- preferential/priority access to resources/facilities;
- preferential/priority routing of emergency telecommunications traffic;
- preferential/priority establishment of emergency telecommunications sessions/calls.

8.4.2 Wireless radio access

Wireless radio access networks are required to support specific mechanisms and capabilities to provide preferential/priority treatment to authorized emergency telecommunications calls/sessions. Technology-dependent mechanisms and capabilities may be used to provide the preferential/priority treatment. This includes, but is not limited to, mechanisms and capabilities for:

- Recognizing emergency telecommunications traffic: This includes identification and marking of authorized emergency telecommunications.
- Preferential/priority access to resources/facilities: This facilitates delivering a request for emergency telecommunications to a NGN when available access resources are scarce.
- Preferential/priority routing of emergency telecommunications traffic: This may include features such as queuing for available resources, exemption from certain restrictive network management functions and reservation of some routes/paths for emergency telecommunications.
- Preferential/priority establishment of emergency telecommunications sessions/calls.

For example, 3GPP specified priority service and multimedia priority service for 3GPP systems. Priority service and multimedia priority service allow authorized users to obtain priority access to the next available radio (voice or data traffic) channels before other users during situations when congestion is blocking call attempts. Priority service supports priority call progression and call completion to support an "end-to-end" priority call from mobile-to-mobile networks, mobile-to-fixed networks, and fixed-to-mobile networks. Multimedia priority service supports priority progression of multimedia sessions and completion to support "end-to-end" priority multimedia sessions, including mobile-to-mobile networks, mobile-to-fixed networks, and fixed-to-mobile networks. Priority service and multimedia priority service for 3GPP systems is specified in [b-3GPP TS 22.153].

Similar to 3GPP, 3GPP2 specified multimedia priority service (MMPS) for 3GPP2 systems. The 3GPP2 specification for MMPS is [b-3GPP2 S.R0117-0-v1.0].

8.4.3 Fixed access

Fixed access networks are required to support specific mechanisms and capabilities to provide preferential/priority treatment to authorized emergency telecommunications calls/sessions. Technology-specific mechanisms (e.g., 802.1p with xDSL, IPCablecom, Packet Cable 2) mechanisms and capabilities may be used to provide the preferential/priority treatment. This includes, but is not limited to, mechanisms and capabilities for:

- Recognizing emergency telecommunications traffic: This includes identification and marking of authorized emergency telecommunications.
- Preferential/priority access to resources/facilities: This facilitates delivering a request for emergency telecommunications to a NGN when available access resources are scarce.
- Preferential/priority routing of emergency telecommunications traffic: This may include features such as queuing for available resources, exemption from certain restrictive network management functions and reservation of some routes/paths for emergency telecommunications.
- Preferential/priority establishment of emergency telecommunications calls/sessions.

For example, [ITU-T J.260] defines requirements for preferential telecommunications over IPCablecom networks. The essential aspects of preferential telecommunications over IPCablecom that [ITU-T J.260] includes are grouped into two areas: prioritization and authentication. These two areas include capabilities to support telecommunications in IPCablecom that may require preferential treatment (e.g., TDR and ETS). The implementation of priority and authentication is necessary for the support of preferential telecommunications in IPCablecom networks.

9 Mechanisms and capabilities supporting some aspects of early warning in NGN

9.1 General

Alert systems used for early warning may be classified as either push or pull models.

The push model relies on participants registering their contact information (e.g., an email address) to a central service. When an event occurs, these registered participants are alerted to the event with potentially more pointers to additional information. A key architectural design in this model is that a central authority determines if information is to be disseminated, and what that information entails. The strength in this model is that it takes on the burden of being active in monitoring events, thus allowing users to continue in their normal responsibilities and remain passive concerning the monitoring of potential disasters or emergencies.

The push model represents a "one" to "many" distribution mechanism, and is enabled at both the service and transport stratum (e.g., multicast).

The pull model is the opposite of the push model in that the former relies on a query-response exchange of information. While both models rely on registrations by individual participants, the pull model places the responsibility of monitoring and obtaining information onto the individual users. The advantage of this system is that information is only provided on an as-needed or on-demand basis.

In summary, alert systems use existing applications and underlying capabilities found in IP-based networks. The addition of pull or push helps make these systems more symbiotic to the needs and expectations of users. The application of each type of alert system can also be used in tandem: the push model can provide periodic automated monitoring and notification, and the pull model can be used to obtain on-demand specific information.

For examples of push and pull, see Appendix II.

9.2 Common alerting protocol (CAP)

This clause describes the common alerting protocol (CAP) specified in [ITU-T X.1303] that can be used to support early warning applications.

[ITU-T X.1303] specifies a general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. CAP also provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

The CAP provides an open, non-proprietary message format for all types of alerts and notifications. It does not address any particular application or telecommunications method. The CAP format is compatible with emerging techniques, such as web services and the ITU-T fast web services, as well as existing formats including the specific area message encoding (SAME) used for the United States' National Oceanic and Atmospheric Administration (NOAA) Weather Radio and the Emergency Alert System (EAS), while offering enhanced capabilities that include:

- flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- multilingual and multi-audience messaging;
- phased and delayed effective times and expirations;
- enhanced message update and cancellation features;
- template support for framing complete and effective warning messages;

- compatibility with digital encryption and signature capability; and
- facility for digital images and audio.

CAP provides reduction of costs and operational complexity by eliminating the need for multiple custom software interfaces to the many warning sources and dissemination systems involved in all-hazard warning. The CAP message format can be converted to and from the "native" formats of all kinds of sensor and alerting technologies, forming a basis for a technology-independent national and international "warning internet".

The CAP specified in [ITU-T X.1303] is technically equivalent and compatible with the OASIS common alerting protocol, V1.1 standard. [ITU-T X.1303] provides an equivalent ASN.1 specification that permits a compact binary encoding and the use of ASN.1 as well as XML schema definition (XSD) tools for the generation and processing of CAP messages. [ITU-T X.1303] enables existing systems, such as H.323 systems, to more readily encode, transport and decode CAP messages.

10 Service restoration priority

In the event of a network failure or outage, critical services (e.g., emergency services) can be interrupted and may need a higher probability of successful restoration over other services. [ITU-T Y.2172] specifies three levels for restoration priority for services in NGN. It allows for such priority classifications to be used in signalling messages such that the service in question can get call/session setup with the desired restoration priority, thus allowing critical services to have a higher probability of successful restoration over other services.

11 Security

The network elements, systems, resources, data, and services used to support emergency telecommunications can be targeted for cyber attacks. The integrity, confidentiality, and availability of emergency telecommunications, especially when under attack, will depend on the security services and practices implemented in the NGN and on the security capabilities (e.g., user authentication and authorization functions) implemented as part of the application service for emergency telecommunications. General guidelines to consider for emergency telecommunications security planning include (but are not limited to):

- All aspects of emergency telecommunications including the signalling and control, bearer/media, and management related data and information (e.g., user profile information) need to be protected against security threats. Security threats to emergency telecommunications could occur at various layers (e.g., transport, service control or service support) and in the different network segments (i.e., access, core network, and interconnection interfaces).
- Establishment and enforcement of security policies and practices that are specific to emergency telecommunications services. Mitigation capabilities to provide protection against various security threats should be identified and implemented. Specifically, mitigation capabilities and security practices beyond those needed for general application services should be identified and implemented for emergency telecommunications. This includes security policies to protect management data and stored information (e.g., user profile information) related to emergency telecommunications.
- Implementation and use of procedures to authenticate and authorize users, devices or the combination of user and device to protect against unauthorized access to services, resources and information (e.g., user information in authentication servers and management systems) associated with emergency telecommunications. For example, authentication and authorization functions should be implemented to prevent use of resources dedicated to

emergency telecommunications by unauthorized users in order to prevent denial of service (DoS) and other types of attack.

- Responsibility within each network for security within its domain for communications that traverse multiple network provider domains so that the end-to-end communication can be secured. Since emergency telecommunications may involve communications that traverse different network provider domains of national and international networks (i.e., countries/administrations), security policy, trust relations, methods and procedures for identifying emergency telecommunications traffic, identity management and authentication of users and networks across multiple network administration domains, need establishment and implementation capabilities.

Security planning for emergency telecommunications should consider the recommendations in [ITU-T Y.2701] for NGN security. In addition, the security framework based on the following security dimensions defined in [ITU-T X.805] should also be considered:

- Access control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy.

Appendix I

Emergency telecommunications categories

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

I.1 Individual-to-authority emergency telecommunications

An individual-to-authority emergency telecommunication is initiated from an individual using ordinary national emergency telecommunication capabilities to seek emergency assistance during an individual (personal) emergency, or even during a confined emergency situation. For example, an individual-to-authority call may involve a short dialled number (e.g., 112, 911, etc.) that provides an individual user a connection to an emergency-answering centre. The centre can dispatch the proper responders (e.g., police, firemen, ambulance) on behalf of the calling party. There may be additional information automatically signalled to the call centre such as caller location. Such information can facilitate an even more prompt reaction since sometimes callers cannot or do not have the time or ability to provide this information themselves. This type of communication is usually a one-to-one connection where the initiator interacts primarily with the destination agency. The vast majority of such telecommunications will involve small-scale emergencies (e.g., an individual house on fire) arising from mostly uncorrelated events although large-scale events (e.g., earthquake) can result in many simultaneous correlated connections. (The term individual is meant broadly and should cover every person who needs emergency assistance (covering persons such as citizens, visitors or other inhabitants of a particular place).) The participants in emergency telecommunications can communicate with each other using multiple types of media including voice, video, real-time text and instant messaging.

I.2 Individual-to-individual emergency telecommunications

The individual-to-individual emergency telecommunications category is initiated from a person or device in the general public to an organization. For example, during and immediately after emergency situations, the public urge to communicate with each other is strong. Consequently, there is a higher demand for individual-to-individual telecommunications at the same time telecommunication resources may be reduced due to damage stemming from emergency events. Considering all these factors, telecommunication networks can congest.

I.3 Authority-to-authority emergency telecommunications

The authority-to-authority emergency telecommunication typically involves an authorized emergency telecommunication user (or his organization) initiating action with another authorized user to:

1) facilitate emergency recovery operations (e.g., by creating emergency control centres and associated administrative controls for resource assistance from government and/or other organizations);
2) restore an essential community infrastructure (e.g., restoring essential water services, electricity, etc.); and
3) initiate measures to enable long-term full recovery (e.g., rebuilding of roads, bridges, buildings, etc.).

Historically, authority-to-authority (sometimes referred to as public safety telecommunications) emergency telecommunications using public networks simultaneously occur when telecommunications resources are congested due to increased individual-to-individual telecommunications.

Given the immense potential of authority-to-authority emergency telecommunications to facilitate restoring a state of normality and to avoid further risk to people or property, this emergency

telecommunication category may be given priority status over other emergency telecommunication categories during times of declared emergencies or the escalations of these.

I.4 Authority-to-individual emergency telecommunications

Finally, authority-to-individual emergency telecommunications (sometimes categorized as early warning systems) typically involve information intended for the public which comes from an authorized source. The content can be information intended for a disaster affected community, such as safety, instructions, guidelines, advice etc. Usually, a particular telecommunication is initiated from one authorized user with many individuals as recipients.

Any-to-any: an example of an ETS from any location/device, contacting any other user (ETS or general public) through some measure of preferential support by the communication infrastructure. GETS in the PSTN is a good example, where the preferential service is not ubiquitous and is not constrained to a selective set of end-devices or destinations.

One-to-one: within the context of emergency telecommunications, this one-to-one is considered a subset of the any-to-any case. In this case, the participants are constrained to any two ETS users.

Many-to-one: one manifestation of this model is a client-server architecture of the web, where any user accesses a single well-known location for information. In the PSTN, this model is realized via 11, 112, etc. systems, where sessions within a region are forwarded to a single public service access point (PSAP).

One-to-many: in this model, information is sent from one source to the set of receivers (end-users) choosing to participate in the dissemination of data. In the case of broadcast media, television and radio are excellent examples since receivers only obtain information from the channel they have selected. In the data communication model, one distinguishes one-to-many from broadcast because the latter infers that all nodes receive the message, whether they choose to or not, where as the former implies direct membership of a group.

Appendix II

Example use cases for early warning alert systems

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

II.1 Push model

Both the private and public/government sectors offer alert systems based on the push model. However, this Recommendation only discusses an example from the public sector. An example of the push model from the public/government sector is the emergency information centre from the Washington D.C. (http://alert.dc.gov/eic/site/default.asp) local government. Users register their contact information in the form of an e-mail address, pager, or mobile phone number (either text messaging, or automated voice messaging). The automated voice messaging is equivalent to inverse-911 and all citizens of D.C., with the corresponding landline exchange, are automatically registered with this service. The alert service, as it pertains to email and pagers, is not restricted to just Washington D.C. residents.

II.2 Pull model

The best example of the pull model operating over the Internet is the I-AM-Alive project from Japan (http://www.isoc.org/inet2000/cdproceedings/8l/8l_3.htm, http://www.iaa-alliance.net/en/). I-AM-Alive effort sprung from the Kobe earthquake in 1995 in order to allow people to determine the status and possible location of loved ones that were affected by the earthquake. It acts as an information collection centre for first responders to deposit information they have discovered. Conversely, it is also a distribution centre where friends and relatives can determine if people they know have been hurt by a disaster.

The I-AM-Alive system uses a combination of input from fax, phone, and the web to store information placed by individuals and/or first responders. Subsequent distribution of information is primarily in the form of web pages, though some information can be obtained from well-known phone numbers associated with the system.

Bibliography

[b-3GPP TS 22.153] 3GPP TS 22.153 (06/2008), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Priority Service (Release 9).* <http://www.3gpp.org/FTP/Specs/html-info/22153.htm>

[b-3GPP2 S.R0117-0-v1.0] 3GPP2 S.R0117-0-v1.0 (06/2006), *3rd Generation Partnership Project 2; Multimedia Priority Service (MMPS) for MMD-based Networks – Stage 1 Requirements.* <http://www.3gpp2.org/Public_html/specs/S.R0117-0%20v1.0_060714.pdf>

[b-IETF RFC 2750] IETF RFC 2750 (2000), *RSVP Extensions for Policy Control.* <http://www.ietf.org/rfc/rfc2750.txt?number=2750>

[b-IETF RFC 3265] IETF RFC 3265 (2002), *(SIP)-Specific Event Notification.* <http://www.ietf.org/rfc/rfc3265.txt?number=3265>

[b-IETF RFC 3853] IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP).* <http://www.ietf.org/rfc/rfc3853.txt?number=3853>

[b-IETF RFC 3936] IETF RFC 3936 (2004), *Procedures for Modifying the Resource reSerVation Protocol (RSVP).* <http://www.ietf.org/rfc/rfc3936.txt?number=3936>

[b-IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework.* <http://www.ietf.org/rfc/rfc4032.txt?number=4032>

[b-IETF RFC 4190] IETF RFC 4190 (2005), *Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony*. <http://www.ietf.org/rfc/rfc4190.txt?number=4190>

[b-IETF RFC 4320] IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction.* <http://www.ietf.org/rfc/rfc4320.txt?number=4320>

[b-IETF RFC 4495] IETF RFC 4495 (2006), *A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow*. <http://www.ietf.org/rfc/rfc4495.txt?number=4495>

[b-IETF RFC 4916] IETF RFC 4916 (2007), *Connected Identity in Session Initiation Protocol*. <http://www.ietf.org/rfc/rfc4916.txt?number=4916>

[b-IETF RFC 5027] IETF RFC 5027 (2007), *Security Preconditions for Session Description Protocol (SDP) Media Streams.* <http://www.ietf.org/rfc/rfc5027.txt?number=5027>

[b-IETF RFC DSCP] draft-ietf-tsvwg-admitted-realtime-dscp-00, *DSCP for Capacity-Admitted Traffic*.

[b-IETF RFC RSVP] draft-ietf-tsvwg-emergency-rsvp, *Resource ReSerVation Protocol (RSVP) Extensions for Emergency Services*.

[b-UN Global Survey] United Nations/International Strategy for Disaster Reduction, *Final Report on a "Global Survey of Early Warning Systems"*, September 2006. (Reference: http://www.unisdr.org/ppew/info-resources/ewc3/Global-Survey-of-Early-Warning-Systems.pdf)

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, 2009