International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2205

(05/2011)

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 International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	**Y.2200–Y.2249**
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

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 can optionally 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.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2205	2008-09-12	13
2.0	ITU-T Y.2205	2011-05-20	13

Keywords

Architecture, early warning (EW), emergency telecommunications, emergency telecommunications service (ETS), NGN, preferential telecommunications, 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/.

Table of 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. The term preferential telecommunications is used in some ITU-T Recommendations to include services that require priority treatment. Emergency telecommunications service is one category of services that is considered to have preferential treatment. The two terms, preferential telecommunications and emergency telecommunications are used interchangeably.

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 can optionally 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; all 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.

2.1 ITU-T

[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 G.808.1] Recommendation ITU-T G.808.1 (2010), *Generic protection switching – Linear trail and subnetwork protection*.

[ITU-T G.841] Recommendation ITU-T G.841 (1998), *Types and characteristics of SDH network protection architectures.*

[ITU-T G.842] Recommendation ITU-T G.842 (1997), *Interworking of SDH network protection architectures.*

[ITU-T G.873.1] Recommendation ITU-T G.873.1 (2006), *Optical Transport Network (OTN): Linear protection.*

[ITU-T G.983.1] Recommendation ITU-T G.983.1 (2005), *Broadband optical access systems based on Passive Optical Networks (PON).*

[ITU-T G.8031] Recommendation ITU-T G.8031/Y.1342 (2009), *Ethernet linear protection switching.*

[ITU-T G.8032] Recommendation ITU-T G.8032/Y.1344 (2010), *Ethernet ring protection switching.*

[ITU-T G.8131] Recommendation ITU-T G.8131/Y.1382 (2007), *Linear protection switching for transport MPLS (MPLS-TP) networks.*

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

[ITU-T H.248.81] Recommendation ITU-T H.248.81 (2011), *Gateway control protocol: Guidelines on the use of the international emergency preference scheme (IEPS) call indicator and priority indicator in ITU-T H.248 profiles.*

[ITU-T H.323] Recommendation ITU-T H.323 (2009), *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 I.630] Recommendation ITU-T I.630 (1999), *ATM protection switching.*

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

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

[ITU-T J.262] Recommendation ITU-T J.262 (2009), *Specifications for authentication in preferential telecommunications over IPCablecom2 networks*.

[ITU-T J.263] Recommendation ITU-T J.263 (2009), *Specification for priority in preferential telecommunications over IPCablecom2 networks*.

[ITU-T Q.812] Recommendation ITU-T Q.812 (2004), *Upper layer protocol profiles for the Q and X interfaces*.

[ITU-T Q.1741.6] Recommendation ITU-T Q.1741.6 (2009), *IMT-2000 references to Release 8 of GSM-evolved UMTS core network.*

[ITU-T Q.3303.3] Recommendation ITU-T Q.3303.3 (2008), *Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Diameter.*

[ITU-T Q.3321.1] Recommendation ITU-T Q.3321.1 (2010), *Resource control protocol No. 1, version 2 – Protocol at the Rs interface between service control entities and the policy decision physical entity.*

[ITU-T Q-Sup.57] ITU-T Q-series Recommendations – Supplement 57 (2008), *Signalling requirements to support the emergency telecommunications service (ETS) in IP networks.*

[ITU-T X.660] Recommendation ITU-T X.660 (2008) | ISO/IEC 9834-1:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree.*

[ITU-T X.674] Recommendation ITU-T X.674 (2011), *Procedures for the registration of arcs under the Alerting object identifier arc.*

[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.1720] Recommendation ITU-T Y.1720 (2006), *Protection switching for MPLS networks.*

[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 (2010), *Functional requirements and architecture of next generation networks.*

[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 (2009), *Requirements and capabilities for ITU-T NGN*.

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

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

[ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

[ITU-T Y.2721] Recommendation ITU-T Y.2721 (2010), *NGN identity management requirements and use cases*.

[ITU-T Y.2722] Recommendation ITU-T Y.2722 (2011), *NGN identity management mechanisms*.

2.2 IETF

[IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[IETF RFC 3168] IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP*.

[IETF RFC 3246] IETF RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behavior)*.

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP)*.

[IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[IETF RFC 4340] IETF RFC 4340 (2006), *Datagram Congestion Control Protocol (DCCP)*.

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

[IETF RFC 4542] IETF RFC 4542 (2006), *Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite*.

[IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes*.

[IETF RFC 5865] IETF RFC 5865 (2010), *A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic*.

2.3 ETSI

[ETSI TS 183 017] ETSI TS 183 017 V3.2.1 (2010), TISPAN *Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification*.

2.4 Broadband Forum

[BBF TR-058] Broadband Forum TR-058 (2003), *Multi-Service Architecture and Framework Requirements*.

[BBF TR-059] Broadband Forum TR-059 (2003), *DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services*.

[BBF TR-101] Broadband Forum TR-101 (2011), *Migration to Ethernet-Based DSL Aggregation*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 alert [ITU-T X.674]: A warning or alarm message concerning an impending danger or problem.

3.1.2 alerting agency [ITU-T X.674]: A national, regional or international entity responsible for the management of alerts.

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

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 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.

3.2.2 preferential telecommunications: A category of services for which premium access to, and/or use of telecommunications network resources is provided.

3.2.3 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:

AAA	Authentication, Authorization, and Accounting
AF	Application Function
ANMS	Access Node Management System
APS	Automatic Protection Switching
AQM	Active Queue Management
ASN	Access Service Network
ASN.1	Abstract Syntax Notation One
BNG	Broadband Network Gateway
BS	Base Station
CAC	Call Admission Control
CAP	Common Alerting Protocol
CPE	Customer Premises Equipment
DCCP	Data Congestion Control Protocol
DoS	Denial of Service
DSCP	Diff-Serv Code Points
DSLAM	Digital Subscriber Line Access Multiplexer
EAS	Emergency Alert System
ECN	Explicit Congestion Notification

EF	Expedited Forwarding
E-MTA	Embedded Multi-Terminal Adapter
ENI	ETS National Implementation
ET	Emergency Telecommunications
ETH	Ethernet Layer Network
ETS	Emergency Telecommunications Service
EW	Early Warning
GETS	Government Emergency Telecommunications Service
IEPS	International Emergency Preference Scheme
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LSP	Label Switched Path
MDF	Main Distribution Frame
MMPS	Multimedia Priority Service
MPS	Multimedia Priority Service
MPLS	MultiProtocol Label Switching
MS	Multiplex Section
NID	Network Interface Device
NOAA	National Oceanic and Atmospheric Administration
NGN	Next Generation Network
ODUk	Optical channel Data Unit k
OLT	Optical Line Termination
OMCI	ONT Management and Control Interface
ONT	Optical Network Termination
OTN	Optical Transport Network
P-CSC-FE	Proxy Call Session Control Functional Entity
PCC	Policy and Charging Control
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PF	Policy Function
PHB	Per Hop Behaviour
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PON	Passive Optical Network
POTS	Plain Old Telephone Service
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
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNC	SubNetwork Connection
SNCP	SubNetwork Connection Protection
SS7	Signalling System No.7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDR	Telecommunications for Disaster Relief
T-MPLS	Transport MPLS
UDP	User Datagram Protocol
UE	User Equipment
UN/ISDR	United Nations International Strategy for Disaster Reduction
USI	Universal Services Interface
VC	Virtual Channel
VLAN	Virtual LAN
VoIP	Voice over IP
VP	Virtual Path
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 and 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.

As noted in the introduction, some ITU-T Recommendations, specifically the ITU-T J.26x-series uses the term preferential telecommunications to include services that require special handling relative to other services. Except in the context of J.26x-series of ITU-T Recommendations, the term preferential telecommunications is not referenced in this Recommendation. The term preferential telecommunications in ITU-T J.26x-series of Recommendations includes ETS, TDR and EW.

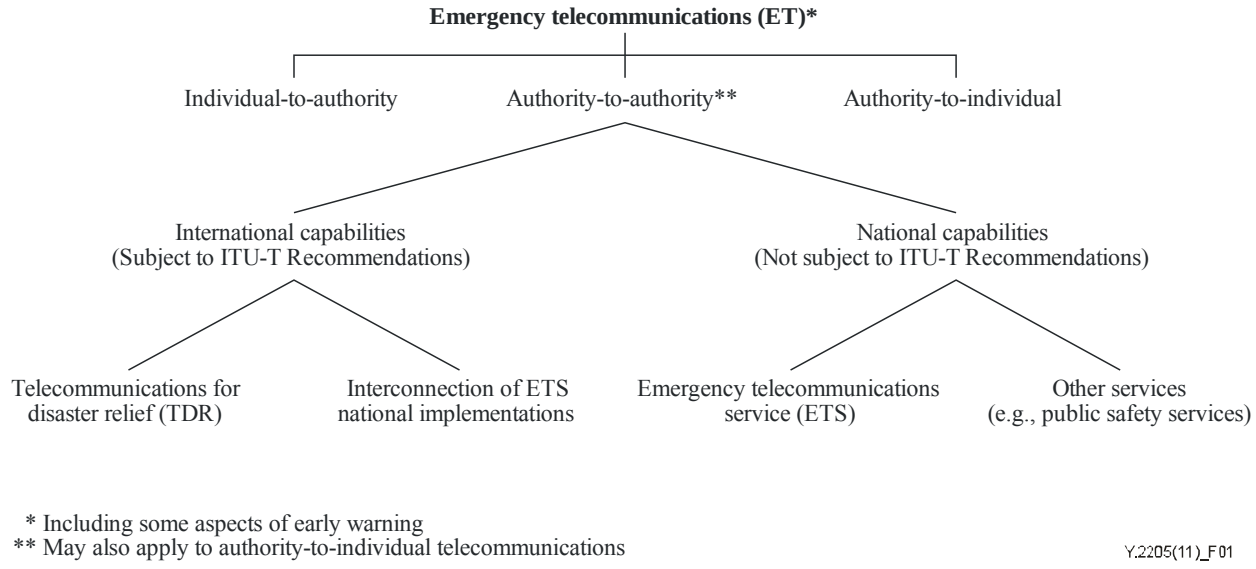

Figure 1 – Terminological relationship framework for emergency telecommunications

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, or local specific and are subject to national or 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" 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 and 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 the 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 the features and mechanisms of an NGN that may be used to facilitate the requirements of emergency telecommunications and some aspects of early warning. However, in considering the protocols, mechanisms and support for emergency telecommunications, it is desirable to avoid introducing features or requirements, though useful, as they may add complexity without significant benefit. Care must be taken by taking into account the overhead incurred in resource consumption and other effects before adding, for example, new features for "priority".

7 General functional requirements and capabilities

Functional requirements and capabilities include those specified in [ITU-T Y.1271] and [ITU-T Y.2201] for 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.

Emergency telecommunications specific network functions can be divided into the following categories: service invocation, authentication and authorization, end-to-end priority treatment, network interconnection and protocol interworking.

A service invocation pertains to user interaction with the user element (e.g., telephone) and the network with information that indicates an emergency telecommunications service request to the service provider network. There are different approaches including subscription arrangements for recognizing the request. Subscription information is used to authorize some service requests.

Authentication and authorization is performed by the service provider to allow or deny the user access to the invoked service for emergency telecommunications. The authorization itself is expected to occur at the core network.

End-to-end priority treatment is a set of capabilities used by the network(s) in providing high probability in establishing and maintaining the service from the originating network to the terminating network including any transit networks. The priority treatment persists with the service invocation to release of the service. The priority treatment is included in admission control and allocation of network resources, and transport of signalling and media bearer packets by the network elements supporting the service.

Network interconnection and protocol interworking is necessary for supporting end-to-end priority treatment for signalling and media transport traversing multiple networks belonging to different providers using different technologies. As an example, the levels of priority may vary depending on the technology used in the multiple networks and mapping from a level defined in one technology to another may be required.

7.2 Early warning

Early warning systems need an effective communication system that is reliable and robust. Some objectives for early warning systems in the context of the NGN as the communication system are to*:*

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

In order to provide warning messages only to those possibly affected by an impending disaster, early warning systems may have objectives related to the filtering of messages so that these reach a selected:

- group of users;
- region or geographical area, etc.

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

8 General security guidelines and requirements

8.1 General guidelines

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 and 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 to be established and implemented.

Additional information can be found in [b-ATIS-1000010].

8.2 General requirements

The security recommendations in [ITU-T Y.2701], [ITU-T Y.2702], and [ITU-T Y.2704], and the identity management (IdM) recommendations in [ITU-T Y.2720], [ITU-T Y.2721], and [ITU-T Y.2722] are relevant to emergency telecommunications security.

8.2.1 Access control

Only authorized users must be allowed access to emergency telecommunications and any associated resources. Any unauthorized access, such as that by intruders masquerading as authorized users, must be prevented.

8.2.2 Authentication

Mechanisms and capabilities to identify, authenticate and authorize access of the emergency telecommunications user, device or user and device combination as applicable based on policy[1] and the assurance level for specific service (e.g., voice, data, video) is necessary for security protection.

8.2.3 Confidentiality and privacy

Confidentiality and privacy protection of emergency telecommunications and end-user information are necessary. This includes confidentiality and privacy protection of emergency telecommunications signalling, control and bearer traffic, end-user information (e.g., identity, subscription and location information) and activity, as applicable.

8.2.4 Communication security

Protection of emergency telecommunications against intrusions is necessary (e.g., prevention of unlawful interception, hijacking or replay of signalling or bearer traffic).

8.2.5 Data integrity

Integrity protection of emergency telecommunications is necessary (e.g., protection against unauthorized modification, deletion, creation, or replay). This includes integrity protection of emergency telecommunications information and any configuration data (e.g., priority marking, priority information stored in policy decision functions, user priority level, etc.).

8.2.6 Availability

Availability of emergency telecommunications must be protected. Specifically, emergency telecommunications and any associated resources must be protected against denial of service (DoS) and other forms of attacks.

9 Mechanisms and capabilities supporting emergency telecommunications in NGN

9.1 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.

---

[1] Policy in this context includes all applicable policies such as those generated from NGN provider decisions, regulatory requirements, or other governmental rules.

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 or sessions. The labels used to identify and mark emergency telecommunications calls or sessions and/or traffic are protocol specific. To achieve specialized (e.g., priority or preferential) treatment end-to-end for all aspects of the emergency telecommunication call or 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 the priority call or 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 protocols in question.

In the transport stratum, the Internet Protocol (IP) may be used. The IP version used may vary from one provider to another and the end-to-end connectivity may require adapting different versions by using, for example, tunneling one version within another. However, this should not impact the transport of emergency telecommunications service-related information.

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 telecommunications call or session can traverse a wide range of transport technologies.

Later clauses will outline the various features and 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), and transport protocols defined by the IETF, it is prudent to utilize applicable IETF-defined capabilities in respect of its usage for the 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 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][2]. 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 an NGN where the service and transport stratum are independent, 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.

9.1.1 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.

In the layered NGN architecture as defined in [ITU-T Y.2012], the priority indicator sent from the service control functions (SCF) to the resource and admission control functions (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.

9.1.2 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 or 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

---

[2] [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."

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).

Example approaches for ETS authentication and authorization are described in Appendix II of [ITU-T Y.2702] and include:

a) Use of personal identification number (PIN): This approach uses a PIN to authenticate the user's authorization to invoke ETS. This approach identifies the user and not the user's device. Therefore, it is normally used in cases where the user is allowed to invoke ETS from any device.

b) Use of subscription/service profile: In this approach, the user device and service profile is provisioned to indicate ETS subscription. When the user device is authenticated as part of the NGN provider (i.e., ETS provider) normal registration and authentication procedures, the user's ETS subscription is identified. When a user initiates an ETS request, the check against the user's service profile determines whether the user device is authorized for the ETS.

c) Use of PIN and service profile combination: These approaches combine the PIN and service profile methods and may be used to concurrently authenticate both the user and the user device to provide higher levels of assurance for ETS.

d) Use of special security tokens and biometrics: In addition to the approaches described above, more sophisticated approaches using special security tokens and biometric capabilities to authenticate and authorize ETS users and terminals may be used to provide a higher level of identity assurances.

Once the user, user device or user and device combination is authenticated and authorized based on the applicable policy, the emergency telecommunications call or sessions are 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 are also necessary to the handing off and receiving of emergency telecommunications calls or sessions 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 the SLAs and applicable policy.

IdM capabilities ([ITU-T Y.2720], [ITU-T Y.2721], and [ITU-T Y.2722]) can be leveraged to provide increased confidence in identity information for emergency telecommunications applications. Appendix III of [ITU-T Y.2721] provides ETS-related IdM use case examples. These use case examples describe how IdM capabilities can be used to support ETS applications and cover the following topics:

- Authentication assurance using device and user combination (e.g., correlation of user and device authentication).
- Enhanced authentication of ETS users for next generation priority services (e.g., use of tokens, digital certificates, voice recognition and biometrics).
- Authentication of called party and data communication sources (e.g., assurance of messages and data sources).
- Identification and authentication of service providers in a multi-provider environment (e.g., identification of access, content and network service providers).
- Single sign-on and single sign-off (e.g., access to multiple application without having to provide credentials individually for each application).

9.1.3 Admission control considerations for higher probability of admission

One of the functions of the resource and admission control function (RACF) is supporting 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 compete), 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). An example of such a mechanism is currently being written within IETF.

9.1.3.1 Call admission control (CAC)

CAC is a set of actions and policies taken by the network at the call or session set-up 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 (voiceband 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 or 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 or 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.

9.2 Service stratum

9.2.1 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 users in another country. In this case, it is important for an ETS call or session which 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).

9.2.2 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 or 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 or session allocations where resources are limited or congested, such as in radio access for wireless networks.

9.2.3 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.

9.2.4 ITU-T H.323 system control protocols

This clause outlines protocols used in the ITU-T 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 ITU-T H.323 priority calls. The ITU-T 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 supports 16 priority levels that can carry the user priority level between the controller and gateway functions. The IEPS call indicator and priority indicator satisfy the ETS requirements of indicating an ETS context and carrying the priority level, respectively. For public safety services, [ITU-T H.248.1] defines the emergency indicator for carrying the priority indication between the controller and gateway functions.

[ITU-T H.248.81] provides guidelines on the use of the IEPS call indicator and priority indicator in ITU-T H.248 profiles for ITU-T H.323 and NGN systems in support of priority services (e.g., ETS).

9.2.5 Diameter

The Diameter protocol [IETF RFC 3588] supports authentication, authorization, and accounting (AAA) for network functions and applications such as network access and IP mobility.

The following attribute value pairs (AVPs) are intended to be used in the Diameter protocol in support of priority services (e.g., ETS):

- MPS-Identifier.
- Reservation-Priority.
- Priority-Level (as part of the allocation retention priority (ARP) AVP).
- Session-Priority.

The MPS-Identifier AVP is defined by 3GPP in [b-3GPP TS 29.214]. The MPS-Identifier is used to mark a priority service (e.g., an ETS/MPS) request over the Rx interface. The MPS-Identifier AVP contains the national variant for the priority service name.

The Reservation-Priority AVP is defined by the European Telecommunications Standards Institute (ETSI) in [ETSI TS 183 017]. [ITU-T Q.3321.1] and [ITU-T Q.3303.3] specify the use of the Reservation-Priority AVP over the resource and admission control function (RACF) Rs and Rw interfaces [ITU-T Y.2111], respectively, in support of priority services. Similarly, [b-3GPP TS 29.214] (Policy and charging control over Rx reference point) and [ITU-T Q.1741.6] specify the Reservation-Priority AVP over the policy and charging control (PCC) Rx interface in support of priority services (e.g., ETS). The Reservation-Priority AVP supports 16 priority levels

that can be used to request priority treatment. Values between 0 and 15 are in increasing order of priority with "15" being the highest and "0" the lowest. The Reservation-Priority AVP includes the priority value of the user.

The Priority-Level AVP (as part of the allocation retention priority (ARP) AVP) is defined by 3GPP in [b-3GPP TS 29.212] (Policy and charging control over Gx reference point) and [ITU-T Q.1741.6]. [ITU-T Q.1741.6] specifies the Priority-Level AVP over the policy and charging control (PCC) Gx interface in support of priority services (e.g., ETS). The Priority-Level AVP supports 15 priority levels that can be used to request priority treatment. Values between 1 and 15 are in decreasing order of priority with "1" being the highest and "15" the lowest. Priority values 1 to 8 are assigned for services that are authorized to receive prioritized treatment (e.g., ETS, MPS). Priority value "0" is spare and treated as a logical error if received. The Priority-Level AVP reflects the priority value of the user.

The Session-Priority AVP is defined in [b-3GPP TS 29.229] (Cx and Dx interfaces based on the Diameter protocol; Protocol details) and [ITU-T Q.1741.6]. [b-3GPP TS 29.229] specifies the use of the Session-Priority AVP over the Cx and Dx interfaces in support of priority services (e.g., ETS). Similarly, [b-3GPP TS 29.329] (Sh interface based on the Diameter protocol; Protocol details) and [ITU-T Q.1741.6] specify the use of the Session-Priority AVP over the Sh interface in support of priority services. The Session-Priority AVP supports 5 priority levels that can be used to request priority treatment over the Cx, Dx, and Sh interfaces. Values between 0 and 4 are defined to be in decreasing order of priority with "0" being the highest and "4" the lowest.

9.3 Transport stratum

9.3.1 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 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 (e.g., as specified within an SLA). The TM Forum has provided guidance on the specification and management of SLAs [b-TM Forum GB917], and, in particular, has considered how such guidance could be applied to ETS.

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 or 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.

9.3.2 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 [IETF RFC 4542] Appendix A. However [IETF RFC 4542] uses the pre-emption technique.

IETF is currently developing extensions to the RSVP that can be used to support an admission priority capability at the network layer to allow a higher probability of session establishment to specific sessions in times of network congestion. 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, these extensions specify 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.

9.3.3 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 recommends 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.

9.3.4 EF DSCP for capacity-admitted traffic

[IETF RFC 5865] defines a VOICE-ADMIT DSCP for a class of traffic that is subject to strict CAC and includes ETS traffic. This would permit real-time traffic conforming to the expedited forwarding (EF) per hop behaviour using a CAC procedure involving authentication, authorization, and capacity admission (see clauses 9.3.1 and 9.3.2 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.

9.3.5 Explicit congestion notification (ECN)

[IETF RFC 3168] defines the dual layer architecture of ECN as one that operates at the network layer (i.e., IP) and the transport layer (e.g., TCP). Its objective is to provide a timely explicit signalled feedback to the source of downstream congestion, but with minimal to no loss of packets, and therefore with minimal disruption of flows. This signalled information is accomplished using intermediate nodes supporting active queue management (AQM), which mark packets with congestion notification and forward them downstream instead of dropping the packet. The end point of the flow then sends feedback indication (i.e., ECN) back to the source via an upper layer transport protocol. [IETF RFC 4340] extended the support of ECN to the data congestion control protocol (DCCP).

In the case of both TCP and DCCP, ECN triggers inherent back-off algorithms that are transparent to applications. The general benefit of this feature is that applications become more net-friendly and reduce the offered load, thereby allowing more users/applications to use the network. In this application-transparency scenario, ECN does not specifically favor ETS users over the general public. Rather, ECN facilitates the continued use of network resources by both ETS and general public users.

The IETF Network Working Group is currently studying how ECN can be used for RTP flows running over UDP/IP which use RTCP as a feedback mechanism. The solution consists of feedback of ECN congestion experienced markings to the sender using RTCP, verification of ECN functionality end-to-end, and how to initiate ECN usage. The current studies within IETF are designed to add ECN support for real-time applications (e.g., voice and video) using RTP/RTCP. In this case, notification of congestion is made available to applications, which may have a variety of reactions to this notification. It can be expected that the default reaction will follow that of TCP and DCCP, wherein the application reduces the offered load onto the network.

9.4 NGN access technology support

9.4.1 General

There are multiple technology-dependent methods for NGN access. According to [ITU-T Y.2012], 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., [b-IEEE 802.11]) and [b-IEEE 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.

In establishing priority treatment for emergency telecommunications, the following aspects are considered: classifying or labelling the traffic for priority treatment, signalling to set up the path for transporting this traffic and mechanisms including the policies to support the requested priority. Some aspects such as the selection of mechanisms, policies and associated implementations are not standardized and may be region specific.

9.4.2 Wireless access

Wireless access networks are required to support specific mechanisms and capabilities to provide preferential/priority treatment to authorized emergency telecommunications calls or 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 calls or sessions.

9.4.2.1 Universal mobile telecommunications system (UMTS) and long term evolution (LTE)

Priority service and multimedia priority service for 3GPP systems is specified in [b-3GPP TS 22.153]. The 3GPP-specified 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 from mobile-to-mobile networks, mobile-to-fixed networks, and fixed-to-mobile networks.

Based on [b-3GPP TS 22.153], 3GPP is developing a Stage 2 Technical Report for enhancements for multimedia priority service (MPS) [b-3GPP TR 23.854] to identify changes to existing Stage 2 3GPP specifications (e.g., [b-3GPP TS 23.401], [b-3GPP TS 23.203], [b-3GPP TS 23.328], and [b-3GPP TS 23.272]) to support MPS, including IP multimedia subsystem (IMS) and policy and charging control (PCC) aspects. This TR is intended to clarify the architectural requirements and call or session flows for MPS. Based on the 3GPP Stage 2 requirements, changes to the existing 3GPP Stage 3 specifications to support MPS for UMTS and LTE access technologies will be specified.

9.4.2.2 Evolution – Data optimized (EV-DO)

Similar to 3GPP, 3GPP2 specified multimedia priority service (MMPS) for 3GPP2 systems. The 3GPP2 specification for MMPS is [b-3GPP2 S.R0117-0]. Several capabilities such as updating of bearer priority levels are included in 3GPP2 systems network interface standards, and these capabilities may be used for providing MMPS. Similarly, several capabilities such as queuing are included in the 3GPP2 systems air interface standards and these capabilities may be used for providing MMPS.

9.4.2.3 WiMAX network access

[b-WFM Stage1-r1] defines the Stage 1 requirements for emergency telecommunications service (ETS) over WiMAX networks for Release 1.6, based on [b-IEEE 802.16] 2009 air interface. [b-WFM Stage1-r2] enhances the Release 1.6 WiMAX ETS Stage 1 requirements for Release 2.0 to support the [b-IEEE 802.16m] air interface.

[b-WFM Stage2-a1] specifies for ETS the Stage 2 WiMAX network solution framework for Release 1.6 to support the Stage 1 requirements. The framework addresses network initiated priority indication and priority treatment for the authentication, authorization, and accounting (AAA) architecture. The ETS framework based on the policy and charging control (PCC) architecture and UE initiated priority mechanisms are being developed for Release 2.0.

[b-WFM Stage3-a1] specifies the Stage 3 WiMAX network procedures and messages for Release 1.6 supporting priority indication and priority treatment, based on the Stage 2 solution framework. A priority indication field is added to the QoS Descriptor parameter of the WiMAX RADIUS and Diameter messages. The priority indication procedures for the network initiated AAA architecture, as well as the priority treatment mechanisms in the BS, ASN gateway, and connectivity service network (CSN) functional entities, are also described in this document. The key areas of ETS support in the WiMAX network are as follows:

1) Upon initial network entry for a UE associated with an ETS enabled WiMAX subscription, priority indications associated with initial service flows for the UE are passed from the authentication, authorization, and accounting (AAA) server to the access service network (ASN) gateway to the base station (BS). The BS applies priority treatment on resource allocation and scheduling for the priority service flows.

2) Upon ETS invocation from a UE, priority indications associated with service flows for the UE are passed from the application function (AF) to the AAA/policy function (PF) server to the ASN gateway to the BS. The BS applies priority treatment on resource allocation and scheduling for the priority service flows.

3) Upon handover, priority indications associated with service flows for the UE are retained from the serving BS to the target BS for intra-ASN handover and from the serving ASN gateway to the target ASN gateway. The BSs apply priority treatment on resource allocation and scheduling on all priority service flows during handover preparation and action.

4) Upon paging to a UE in the idle mode, priority indication associated with the service flow are passed from the ASN gateway with data path function to the anchor paging controller, and then to the BS. The BS applies priority treatment on resource allocation and scheduling for priority service flows in broadcasting paging messages. In response to priority paging, when the UE enters the network, the BS recognizes the incoming ETS call priority and gives priority treatment to the UE for idle mode exit as well as service flow addition/change for the ETS call to the terminating UE.

The additional ETS Stage 3 procedures and messages are being developed for Release 2.0, which include priority indication and treatment for ranging, service flow creation, and universal services interface (USI).

9.4.3 Fixed access

Fixed access networks are required to support specific mechanisms and capabilities to provide preferential/priority treatment to authorized emergency telecommunications calls or sessions. Technology-specific mechanisms (e.g., [b-802.1p] with xDSL, IPCablecom, IPCablecom 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 or sessions.

The technology-specific considerations are described in the following subclauses.

9.4.3.1 IPCablecom network access

[ITU-T J.260] defines the requirements for preferential telecommunications service over IPCablecom networks. [ITU-T J.261] defines the framework for developing the specifications in order to support these requirements over both IPCablecom and IPCablecom 2 networks. The framework addresses two key areas: priority and authentication. Other areas such as provisioning for restorability are identified for future revisions. The framework is defined to include both common aspects as well as differences resulting from the architectures used in IPCablecom and IPCablecom 2 networks (IMS-based). IPCablecom and IPCablecom 2 are packet networks that have the properties discussed in clause 6 such as sharing resources for data and control traffic. The framework in [ITU-T J.261] classifies the priority requirements in [ITU-T J.260] in terms of signalling, labelling and mechanisms.

[ITU-T J.262] defines the specification to support the authentication requirements in IPCablecom 2 networks. Example flows are included in [ITU-T J.262] to show the message exchanges for different scenarios corresponding to PIN-based authentication, use of SIP Resource Priority header: user agent originating a VoIP call to PSTN user using a PIN, user agent originating a VoIP call to another VoIP user agent using a PIN-and subscription-based authentication.

[ITU-T J.263] defines the specification to support the priority signalling for preferential treatment using [IETF RFC 4412] SIP Resource Priority header. Two options are included in the specification: (1) the UA initiates the request including the Resource-Priority header; (2) based on the information in the request, the Resource-Priority header with the appropriate priority level value is inserted by the P-CSC-FE. The namespace and priority level values to be used in different regions are included as annexes to [ITU-T J.263]. In some regions, it is required to support the values defined in [IETF RFC 4412]. [ITU-T J.263] also describes the relationship to service flows that are set up during provisioning of the embedded multi-terminal adapter (E-MTA) at the DOCSIS MAC layer to reflect the required QoS parameters for preferential telecommunications. There is no labelling mechanism identified for the data transfer because RTP does not include markings to indicate priority. Priority enabling mechanisms to reserve resources and perform admission control are supported by setting gates defined as part of dynamic quality of service (DQoS) in IPCablecom.

9.4.3.2 xDSL network access

The Ethernet-based DSL aggregation reference architecture is described in [BBF TR-101]. Policy control in the DSL access network is based on the specifications found in [BBF TR-058] and [BBF TR-059].

The basic approach to providing ETS capabilities in a DSL access network is to use the existing QoS capabilities to provide priority to ETS calls or sessions. The policy server/policy decision point (PDP) is the only "ETS-aware" device in this approach, and it sets the appropriate priority to be applied to flows using existing QoS capabilities in the broadband network gateway (BNG).

Due to the non-blocking nature of the network interface device (NID) and main distribution frame (MDF), no ETS features are required in these network elements. Bandwidth is provisioned and is fixed between the NID and the digital subscriber line access multiplexer (DSLAM), and the DSLAM is also engineered to be non-blocking. Thus, the approach chosen is to use the QoS

capabilities of the BNG to control the flow of the data through the DSLAM to ensure that the traffic does not congest the DSLAM.

The Ethernet aggregation function is engineered to transport all traffic between the BNG and the DSLAM and is, therefore, another non-blocking element.

The customer premises equipment (CPE) access gateway may or may not be ETS aware. If it is ETS aware, then the access gateway may prioritize ETS traffic to ensure transmission into the DSL access network, and to ensure that the DSLAM does not become congested.

The policy server/PDP is responsible for providing the appropriate policy for ETS traffic to the BNG. For ETS, the policy server/PDP implements admission control policies to give an ETS call or session a high likelihood of being successful. The policies affect establishing, maintaining, and terminating the ETS call or session through the DSL access network to the customer premises network. It is assumed that the policy server/PDP will receive the ETS call or session request from the NGN (e.g., proxy call session control functional entity (P-CSC-FE)). The policy server/PDP will recognize the request with the appropriate ETS information and instruct the BNG appropriately to provide priority treatment.

The BNG is responsible for providing priority to ETS traffic. The BNG applies instructions from the policy server/PDP when reserving and establishing appropriate resources for handling an ETS call or session. It applies priority treatment, including marking bearer packets for priority treatment for transmission to the CPE access gateway and to the regional broadband network.

9.4.3.3 Fibre (FTTx) network access

The fibre access passive optical network (PON) reference architecture is described in [ITU-T G.983.1]. The reference architecture refers to an access node management system (ANMS) for control of the optical line termination (OLT) and optical network termination (ONT). The ANMS provides the policy decision point (PDP) functionality that is enforced by the policy enforcement points (PEPs) located in the OLT and ONT.

There is today no direct policy control or policy enforcement within the fibre access network. However, to support ETS priority handling of call or session set-up in the fibre access network, the ANMS will be required to support dynamic policy control functions. The basic approach to providing ETS capabilities in a fibre access network is to use the existing QoS capabilities to provide priority to an ETS call or session. The ANMS (e.g., policy server) is the only "ETS-aware" device in this approach, and it sets the appropriate priority to be applied to flows using the existing QoS capabilities in the OLT and ONT. ETS policy is signalled over the Q3 interface (as specified in [ITU-T Q.812]) to the OLT and is reflected from the OLT to the ONT via the ONT management and control interface (OMCI).

The ANMS is responsible for providing the appropriate policy for ETS traffic to the OLT. For ETS, the ANMS implements admission control policies to give an ETS call or session a high likelihood of being successful. The policies affect establishing, maintaining, and terminating the ETS call or session in the fibre access network. The ANMS makes the final policy decisions and provides sufficient information to make the OLT and ONT perform the resource control operation for ETS. It is assumed that the ANMS will receive the ETS call or session request from the NGN (e.g., proxy call session control functional entity (P-CSC-FE)). The ANMS will recognize the request with the appropriate ETS information and instruct the OLT appropriately to provide priority treatment.

The OLT and ONT are engineered to transport all ETS traffic. The OLT is responsible for providing priority to ETS traffic. The OLT applies instructions from the ANMS when reserving and establishing appropriate resources for handling an ETS call or session. It applies priority treatment, including marking bearer packets for priority treatment for transmission.

10 End-to-end support for emergency telecommunications

Figure 2 shows an end-to-end call or session matrix for supporting various ETS call or session flows. It illustrates calls or sessions:

- originating and terminating on IP (e.g., Cable and DSL), narrow-band wireline (e.g., POTS phone), and wireless (e.g., GSM and CDMA phone) access; and
- traversing through IP and circuit-switched (TDM) core networks.

Support of the end-to-end ETS requires the interworking of ETS specific information between the IP technology domain and other technology domains (e.g., wireless or wireline TDM domains). This includes the necessary interworking for the end-to-end ETS call or session that may cross different technology domains shown in Figure 2. For example, the ETS specific information (e.g., ETS call marking, priority level) needs to be signalled across the network-to-network interface (NNI) between interconnecting NGN providers.

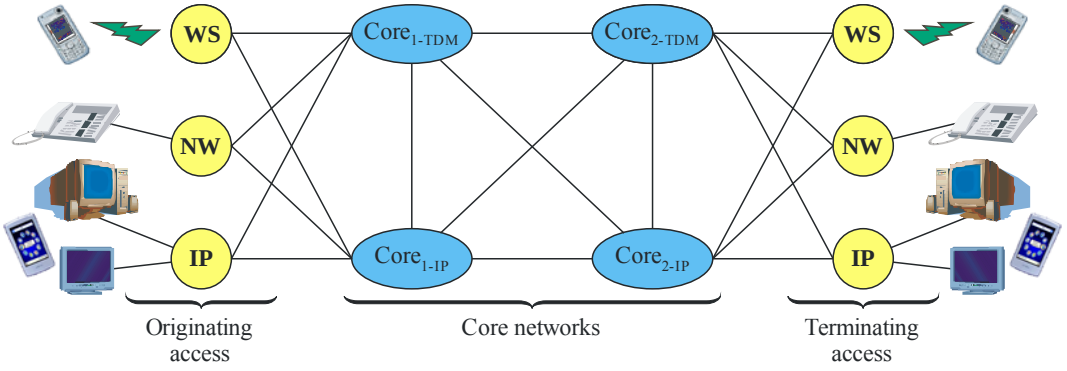

Figure 2 – End-to-end call or session matrix

The call or session scenarios associated with Figure 2 can be found in [b-ATIS-1000010]. [b-ATIS-1000010] defines the procedures and capabilities required to support ETS within and between IP-based service provider networks. The following call or session scenarios are possible based on the matrix shown in Figure 2:

– Originating access to core network 1
  - Originating wireline access to IP core network
  - Originating wireless access to IP core network
  - Originating IP access to IP core network
  - Originating IP access to TDM core network

– Core 1 network to core 2 network
  - TDM core network to IP core network
  - IP core network to TDM core network
  - IP core 1 network to IP core 2 network

– Core 2 Network to terminating Access
  - IP core network to wireline terminating access
  - IP core network to wireless terminating access
  - IP core network to IP terminating access
  - TDM core network to IP terminating access

Setting up the ETS call or session requires careful implementation of the necessary signalling protocols that convey the required information signifying the critical nature of ETS. In order to support end-to-end priority treatment, it is important to support the mapping of priority information to facilitate seamless protocol interworking between the different protocols used within a network (e.g., vertical protocol interworking between call or session control and bearer control) or between different network types (e.g., call or session control interworking between two networks) including PSTN. Similarly, it is critical to allow mapping of priority information to facilitate seamless interworking between the different transport types, i.e., media types. Without such an interworking/mapping, end-to-end priority treatment may not be achievable.

ITU-T is currently preparing guidance for mapping required signalling protocol attributes (ETS priority information) to support the proper set-up and admission of ETS for various "horizontal" (e.g., ISUP, SIP, ITU-T H.225.0) and "vertical" (e.g., ITU-T H.248.0, Diameter).

[ITU-T Q-Sup.57] provides signalling requirements to support preferential capabilities within IP networks for the ETS. An example call flow from [ITU-T Q-Sup.57] illustrating successful authentication and set-up of ETS call or session is provided in Appendix III.

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

11.1 General

Alert systems used for early warning may be classified by whether they employ a push or pull models.

The push model relies on participants registering their contact information (e.g., an e-mail 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.

11.2 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. CAP uses the extensible markup language (XML) and provides standard data interchange formats for structured information.

[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
- the facility to transmit 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. OASIS also specified CAP V1.2 providing updates to CAP V1.1.

[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 ITU-T H.323 systems, to more readily encode, transport and decode CAP messages.

11.3 Procedures for the registration of arcs under the alerting object identifier arc

[ITU-T X.674], "Procedures for the registration of arcs under the Alerting object identifier arc", provides for the registration of object identifier (OID) arcs to identify different kinds of alerts and alerting agencies. Specifically, it specifies the procedures for the registration of arcs to identify (all kinds of) alerts and alerting agencies under the Alerting object identifier arc {joint-iso-itu-t(2) alerting(49)} according to [ITU-T X.660].

[ITU-T X.674] facilitates the allocation and use of OIDs to identify alerting agencies (e.g., alerting agencies designated by World Meteorological Organization (WMO) Member States).

NOTE – The WMO maintains a registry of Alerting Authorities. This can be found at: http://www-db.wmo.int/alerting/authorities.html.

12 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 or session set-up with the desired restoration priority, thus allowing critical services to have a higher probability of successful restoration over other services.

13 Protection switching and restoration

13.1 General considerations

A number of general concepts common to many transport technologies are described in [ITU-T G.808.1]. Several important issues to be considered when providing protection for emergency telecommunications traffic are identified in [ITU-T G.808.1].

13.1.1 Individual protection

The individual protection concept applies to those situations where it is useful to protect only a part of the traffic signals which need high reliability.

13.1.2 Group protection

This allows protection switching through the treatment of a logical bundle of transport entities as a single entity after the commencement of protection actions.

13.1.3 Architectural types

The following architecture types are identified in [ITU-T G.808.1] and are summarized below.

13.1.3.1 1+1 protection architecture

In the 1+1 architecture type, a protection transport entity is dedicated as a backup facility to the working transport entity.

13.1.3.2 1:n protection architecture

In the 1:n architecture type, a dedicated protection transport entity is a shared backup facility for n working transport entities.

13.1.3.3 m:n protection architecture

In the m:n architecture type, m dedicated protection transport entities share backup facilities for n working transport entities, where $m \leq n$ typically.

13.1.4 Switching types

The protection switching types can be a unidirectional switching type or a bidirectional switching type.

It should be noted that all switching types, except 1+1 unidirectional switching, require a communications channel between the two ends of the protected domain; this is called the automatic protection switching (APS) channel.

A list of advantages/disadvantages of applying switching types to all the cases above is given in [ITU-T G.808.1].

In the context of an IP-based emergency telecommunications, unidirectional switching may be adequate since, in general, the paths in each direction are not directly associated due to the nature of unidirectional nature of paths/routing through IP-based networks.

13.1.5 Operation types

The protection operation types can be a non-revertive operation type or a revertive operation type.

In revertive operation, the traffic signal (service) always returns to (or remains on) the working transport entity when it has recovered from the defect.

In non-revertive operation, the traffic signal (service) does not return to the original working transport entity.

It is noted in [ITU-T G.873.1] 1+1 protection is often provisioned as non-revertive, as the protection is fully dedicated in any case, and this avoids a second "glitch" to the traffic. There may, however, be reasons to provision this to be revertive (e.g., so that the traffic uses the "short" direction around a ring except during failure conditions. Certain operator policies also dictate revertive operation even for 1+1).

13.2 SDH protection architectures

[ITU-T G.841] provides the necessary equipment-level specifications to implement different choices of protection architectures for synchronous digital hierarchy (SDH) networks.

Protected entities may range from a single SDH multiplex section (e.g., linear multiplex section protection), to a portion of an SDH end-to-end path (e.g., subnetwork connection protection), or to an entire SDH end-to-end path. Physical implementations of these protection architectures may include rings or linear chains of nodes. Each protection classification includes guidelines on network objectives, architecture, application functionality, switching criteria, protocols, and algorithms.

Additionally, [ITU-T G.842] provides specifications for the interworking of network protection architectures. Specifically covered are single and dual node interconnection between MS-shared protection rings and subnetwork connection protection (SNCP) rings of the same or different types.

13.3 Optical transport network (OTN)

[ITU-T G.873.1] defines the automatic protection switching (APS) protocol and protection switching operation for the linear protection schemes for the optical transport network at the optical channel data unit (ODUk) level.

The protection schemes considered in [ITU-T G.873.1] are:

- ODUk subnetwork connection protection with inherent monitoring (1+1, 1:n);
- ODUk subnetwork connection protection with non-intrusive monitoring (1+1);
- ODUk subnetwork connection protection with sublayer monitoring (1+1, 1:n).

For a given direction of transmission, the "head end" of the protected signal is capable of performing a bridge function, which will place a copy of a normal traffic signal onto a protection entity when required. The "tail end" will perform a selector function, where it is capable of selecting a normal traffic signal either from its usual working entity, or from a protection entity. In the case of bidirectional transmission, where both directions of transmission are protected, both ends of the protected signal will normally provide both bridge and selector functions.

13.4 Ethernet linear protection switching

[ITU-T G.8031] describes the specifics of protection switching for Ethernet VLAN signals. Included are details pertaining to Ethernet layer network (ETH) protection characteristics, architectures and the APS protocol.

Linear 1+1 and 1:1 protection switching architectures with unidirectional and bidirectional switching are defined in [ITU-T G.8031].

In the linear 1+1 protection-switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

Although selection is made only at the sink of the protected domain in linear 1+1 protection switching architecture, bidirectional 1+1 protection switching needs APS coordination protocol so that selectors for both direction selects the same entity. On the other hand, unidirectional 1+1 protection switching does not need APS coordination protocol.

In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic. Since source and sink need to be coordinated to ensure that the selector bridge at the source and the selector at the sink select the same entity, APS coordination protocol is necessary.

13.5 Ethernet ring protection switching

[ITU-T G.8032] defines the automatic protection switching (APS) protocol and protection switching mechanisms for ETH layer Ethernet ring topologies. Included are details pertaining to Ethernet ring protection characteristics, architectures and the ring APS protocol.

The protection protocol defined in [ITU-T G.8032] enables protected point-to-point, point-to-multipoint and multipoint-to-multipoint connectivity within the ring or interconnected rings, called "multi-ring/ladder network" topology.

13.6 Linear protection switching for transport MPLS (T-MPLS)

[ITU-T G.8131] provides requirements and mechanisms for end-to-end trail and subnetwork connection (SNC) protection switching for transport MPLS (T-MPLS) networks. It describes the trail protection and SNC protection architectures types, the uni- and bidirectional switching types and the revertive and non-revertive operation types. It defines the automatic protection switching (APS) protocol used to align both ends of the protected domain.

[ITU-T G.8131] specifies 1+1 architecture and 1:1 architecture. The 1+1 architecture operates with unidirectional switching. The 1:1 architecture operates with bidirectional switching.

13.7 ATM protection switching

[ITU-T I.630] provides architectures and mechanisms for protection switching at the ATM layer. The architecture includes the extent of the protected domain and arrangement of protected domain. The resource for protection entities is pre-allocated. The mechanism includes a protection switching trigger, hold-off mechanisms and protection switching control protocol.

[ITU-T I.630] describes individual VP/VC protection and group protection. The individual VP/VC protection is a technique where a single network or subnetwork connection is used for working entity and protection entity. The group protection is a technique where a logical bundle of one or more network or subnetwork connections is used for the working entity and protection entity.

Currently, [ITU-T I.630] describes 1+1 and 1:1 bidirectional protection switching as well as 1+1 unidirectional protection switching.

13.8 Protection switching for MPLS networks

[ITU-T Y.1720] provides requirements and mechanisms for 1+1, 1:1, shared mesh, and packet 1+1 protection switching functionality for the user-plane in MPLS layer networks. The mechanism defined herein is designed to support end-to-end point-to-point LSPs.

[ITU-T Y.1720] is developed to specify protection switching techniques. [ITU-T Y.1720] explains the difference between protection switching and re-routing as follows:

Protection switching: This implies that both routing and resources are pre-calculated and allocated to a dedicated protection LSP prior to failure. Protection switching, therefore, offers a strong assurance of being able to re-obtain the required network resources post failure.

Re-routing: This implies that a dedicated protection LSP is not defined, and so neither routing nor resources are pre-calculated or allocated prior to failure. Re-routing is commonly used to refer to cases where there are routing and signalling functions in operation, and that when a "re-connection request" has to be instigated on failure (either by the network, or by the customer), that this "reconnect request" has to contend with other similar traffic types for obtaining the required resource. Re-routing, therefore, offers no assurance of being able to re-obtain the required network resources post-failure and is generally slower than protection switching.

Protection switching is necessary for fast recovery from failure, and thereby enhances the reliability and availability performance of MPLS networks.

For protection switching, the following features are required:

1) Protection switching should be applied to an entire LSP.
2) Prioritized protection between signal fail and operator switch requests.
3) The possibility to achieve protection at the MPLS layer as fast as possible (subject to the temporal resolution of the defect detection mechanism) should be provided.
4) Protection ratio of 100%, i.e., 100% of impaired working traffic is protected for a failure on a single working LSP.
5) An extra traffic capability should be supported, when possible.

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., an 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 while 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/her 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 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 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 may include 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 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 911, 112, etc., systems, where sessions within a region are forwarded to a single public safety answering 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, whereas 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 or 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 or government sector is the emergency information centre from the Washington D.C. (http://alert.dc.gov/eic/site/default.asp) local government website. 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 e-mail 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.

Appendix III

Example ETS call/session flows for NGN

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

This appendix provides an example ETS call or session flow from [ITU-T Q-Sup.57] that is applicable to NGN. This call flow illustrates a successful ETS call or session set-up where the authentication and authorization of the user utilizes a PIN.

Figure III.1 illustrates an ETS user authentication method that utilizes a PIN entered by the user in an IP network. A media server (MS) is a combination of media resource control functional entity/media resource processing functional entity (MRC-FE/MRP-FE). All SIP requests include resource-priority header (RPH) [IETF RFC 4412] to indicate that priority treatment is required.

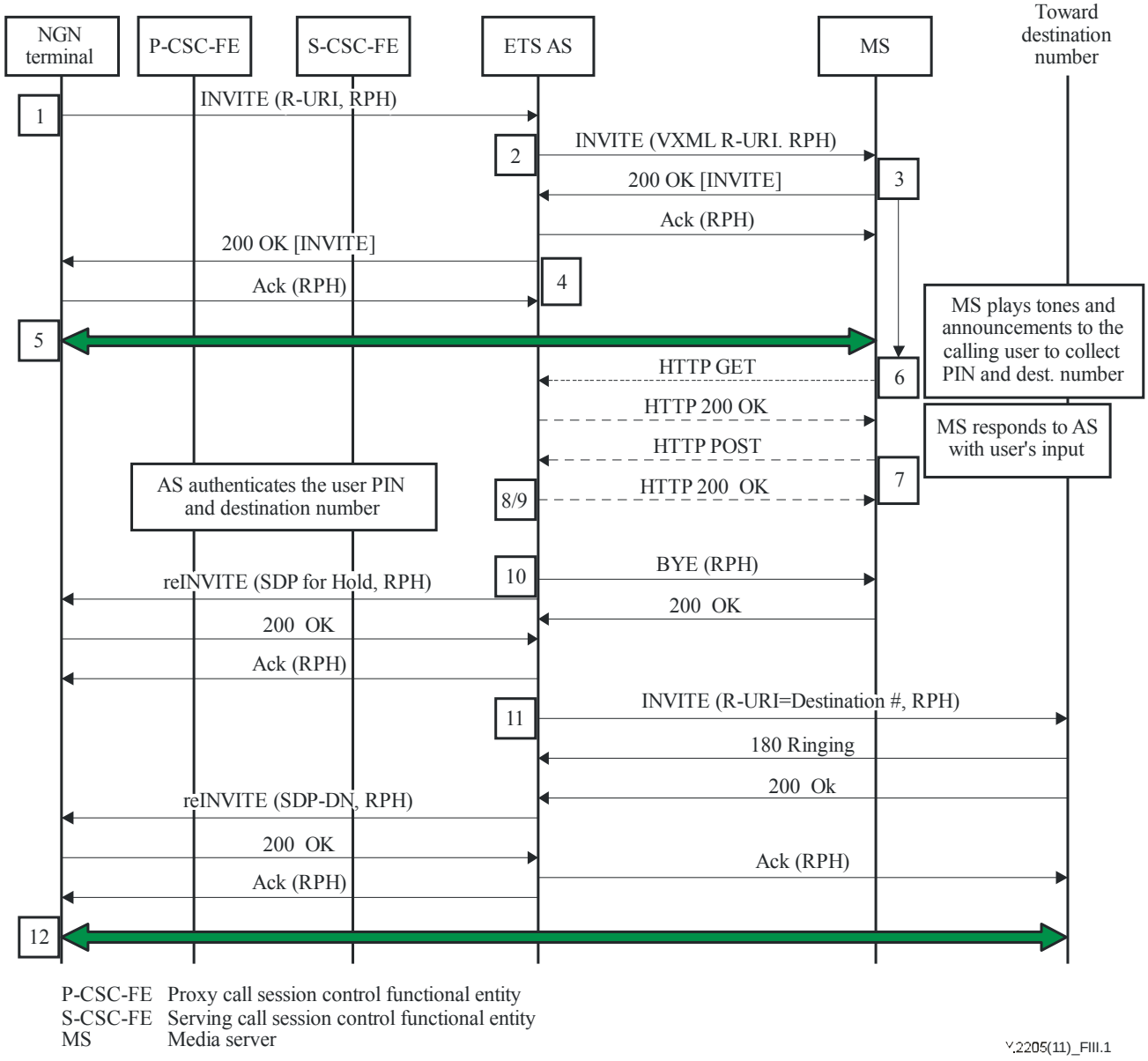

Figure III.1 – ETS call or session set-up using PIN authentication

1) The call or session is routed to an ETS application server (AS) where user authentication processing is initiated.

2) The ETS AS sends an INVITE message to the selected media server (MS), with an SDP offer associated with the caller. The INVITE message contains the URL of a VoiceXML script, stored at the ETS AS. The script describes how the MS should interact with the caller (what announcement to play, how to collect digits, how many digits to collect, inter-digit timers, etc.).

3) Upon receipt of the INVITE message, the MS:

   - May send a 100 Trying to the ETS AS;
   - Retrieves the VoiceXML script directly from the ETS AS using HTTP and the URL in the INVITE message (MS sends a HTTP GET to the ETS AS and VoiceXML script is returned from the ETS AS in an HTTP 200 OK);
   - Validates the script;
   - Formulates and sends a 200 OK message containing its own SDP to the ETS AS.

4) The ETS AS sends a 200 OK towards the calling party (NGN terminal), including in it the session information it received from the MS.

5) At this point, the media connection is available between the MS and the calling party.

6) Upon receipt of the ACK and VXML script in the HTTP 200 OK, the MS executes the VoiceXML script. It plays a tone and collects digits (PIN) entered by the calling party.

7) The MS then sends the collected digits directly to the ETS AS using an HTTP POST message.

8) Upon receipt of the collected digits, the ETS AS verifies whether the received digits (PIN) are valid.

   - If the digits received are invalid (number of digits received or the wrong number), the ETS AS determines that further interaction with the caller is required. The ETS AS returns an HTTP 200 OK message to the MS with a new VoiceXML script. The ETS AS will instruct for final handling treatment.
   - If the received digits are valid, the ETS AS will instruct the MS to play the announcement to collect the digits (destination number).

9) The ETS AS determines that the calling party entered destination digits are valid.

10) The ETS AS releases the MS from the call or session with a SIP BYE, and sends a reINVITE toward the calling party, with a SDP to place the media on hold.

11) The ETS AS sends an INVITE toward the destination party. Upon receiving 200 OK (answer), the ETS AS sends a reINVITE with the SDP associated with the destination toward the calling party.

12) The media path is established between the calling party and destination number with the authentication ETS AS in the call control path.

Bibliography

[b-ITU-T Q-Sup.62] ITU-T Q-series Recommendations – Supplement 62 (2011), *Overview of the work of standards development organizations and other organizations on emergency telecommunications service*.

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

[b-ATIS 1000010] ATIS-1000010.2006, *Support of Emergency Telecommunications Service (ETS) in IP Networks*.

[b-IEEE 802.11] IEEE Std 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between system – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[b-IEEE 802.16] IEEE Std 802.16-2009, *IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems*.

[b-IEEE 802.16m] IEEE Std 802.16m-2011, *IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems, Amendment 3: Advanced Air Interface*.

[b-IEEE 802.1p] IEEE Std 802.1D-2004, *IEEE Standard for Local and metropolitan area networks; Media Access Control (MAC) Bridges*.

[b-3GPP TR 23.854] 3GPP TR 23.854 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Enhancements for Multimedia Priority Service (Release 10)*.

[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 8)*.

[b-3GPP TS 23.203] 3GPP TS 23.203 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture (Release 10)*.

[b-3GPP TS 23.272] 3GPP TS 23.272 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Circuit Switched (CS) Fallback in Evolved Packet System (EPS); Stage 2 (Release 10)*.

[b-3GPP TS 23.328] 3GPP TS 23.228 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 10)*.

[b-3GPP TS 23.401] 3GPP TS 23.401 (in force), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 10)*.

[b-3GPP TS 29.212] 3GPP TS 29.212, version 9 6.1 (2011-04), *Universal Mobile Telecommunications System (UMTS);* LTE; *Policy and Charging Control over Gx reference point (Release 9)*.

[b-3GPP TS 29.214] 3GPP TS 29.214 (in force), *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Rx reference point (Release 10)*.

[b-3GPP TS 29.229] 3GPP TS 29.229, version 9.3.0 (2010-10), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (Release 9)*.

[b-3GPP TS 29.329] 3GPP TS 29.329 v9.4.0 (2011-01), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (Release 9)*.

[b-3GPP2 S.R0117-0] 3GPP2 S.R0117-0-v1.0 (06/2006), *3rd Generation Partnership Project 2; Multimedia Priority Service (MMPS) for MMD-based Networks – Stage 1 Requirements*.

[b-IETF RFC 2750] IETF RFC 2750 (2000), *RSVP Extensions for Policy Control*.

[b-IETF RFC 3265] IETF RFC 3265 (2002), *Session Initiation Protocol (SIP) – Specific Event Notification*.

[b-IETF RFC 3853] IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)*.

[b-IETF RFC 3936] IETF RFC 3936 (2004), *Procedures for Modifying the Resource reSerVation Protocol (RSVP)*.

[b-IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework*.

[b-IETF RFC 4190] IETF RFC 4190 (2005), *Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony*.

[b-IETF RFC 4320] IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction*.

[b-IETF RFC 4495] IETF RFC 4495 (2006), *A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow*.

[b-IETF RFC 4916] IETF RFC 4916 (2007), *Connected Identity in Session Initiation Protocol (SIP)*.

[b-IETF RFC 5027] IETF RFC 5027 (2007), *Security Preconditions for Session Description Protocol (SDP) Media Streams*.

[b-TM Forum GB917] TM Forum GB917 (in force), *SLA Management Handbook, Release 3.0*.

[b-WFM Stage 1-r1] WiMAX Forum – WFM-T31-122-R016v01 (2009), *Service Provider Working Group (SPWG) ETS Phase 1 Requirements for Release 1.6*.

[b-WFM Stage 1-r2] WiMAX Forum – WFM-T31-122-R020v01 (2009), *SPWG ETS Requirements, Release 2.0*.

[b-WFM Stage 2-a1] WiMAX Forum – WFM-T32-001-R016v01 (2010), *Network Architecture – Architecture Tenets, Reference Model and Reference Points, Base Specification, Release 1.6,) ETS Stage 2 Specification (Section 7.14)*.

[b-WFM Stage 3-a1] WiMAX Forum – WFM-T33-001-R016v01 (2010), *Network Architecture – Detailed Protocols and Procedures, Base Specification, Release 1.6, ETS Stage 3 Specification (Section 4.19).*

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2012