International Telecommunication Union

Compendium of ITU's work on Emergency Telecommunications

RADIOCOMMUNICATION
TELECOMMUNICATION STANDARDIZATION
TELECOMMUNICATION DEVELOPMENT

Edition 2007

International Telecommunication Union

COMPENDIUM ON ITU'S WORK ON EMERGENCY TELECOMMUNICATIONS

This publication presents, for the first time under one cover, the work being done by ITU's three Sectors (Radiocommunication, Standardization and Telecommunication Development) in the field of emergency telecommunications (or disaster communications). The release of this compendium is timely since disasters are striking with increased frequency and magnitude, resulting in unprecedented loss of human life, not to mention economic disruption and damage.

The publication is comprehensive and contains factual information that is concise and well-organized for easy access, particularly by practitioners in the area of disaster management. It simplifies and demystifies the complex technical issues that characterize the rapidly-evolving field of telecommunications/information and communication technologies, especially in this era of convergence and with the emergence of next-generation networks.

For further information

Please contact:

Mr Cosmas ZAVAZAVA
Telecommunication Development Bureau (BDT)
ITU
Place des Nations
CH-1211 GENEVA 20
Switzerland
Telephone: +41 22 730 5447
Fax: +41 22 730 5484
E-mail: cosmas.zavazava@itu.int

Placing orders for ITU publications

Please note that orders cannot be taken over the telephone. They should be sent by fax or e-mail.

ITU
Sales Service
Place des Nations
CH-1211 GENEVA 20
Switzerland
Fax: +41 22 730 5194
E-mail: sales@itu.int

The Electronic Bookshop of ITU: www.itu.int/publications

International Telecommunication Union

Compendium of ITU's work on Emergency Telecommunications

Edition 2007

Radiocommunication

Telecommunication Standardization

Telecommunication Development

International Telecommunication Union

The following ITU Inter-Sectoral Emergency Communications Team (IECT) compiled and edited this Compendium on ITU's work on Emergency Telecommunications:

Cosmas L. Zavazava:	Volume I on the work of the Telecommunication Development Sector
Fabio Leite:	Volume II on the work of the Radiocommunication Sector
Simão de Campos:	Volume III on the work of the Telecommunication Standardization Sector

International Telecommunication Union
Place des Nations
CH-1211 Geneva Switzerland

Denominations and classifications employed in this publication do not imply any opinion on the part of the International Telecommunication Union concerning the legal or other status of any territory or any endorsement or acceptance any boundary. Where the designation "country" appears in this publication, it covers countries and territories.

Preface

It is with utmost pleasure that I present this edition of the Compendium of ITU Work in Emergency Telecommunications. This is the first time that ITU's work on Emergency Telecommunications in Radiocommunication, Telecommunication Standardization, and Telecommunication Development has been compiled under one cover, making this therefore the most comprehensive publication ever.

Owing to the fast evolving nature of ITU's work in coordinating the effective use of the radio-frequency spectrum as evidenced by the outcome of the just concluded World Radiocommunication Conference (WRC), development of technical standards for telecommunications, and deployment of these technologies to assist countries in their disaster management effort, the release of this publication is timely. Since the Asian tsunami of 2004, disasters have struck with high frequency and greater ferocity resulting in a high increase in demand for ITU assistance. Most recently, ITU had to deploy satellite equipment to Peru in August, Bangladesh in September, and Uganda in October. This has been unprecedented but gives us the impetus to intensify our work in this area.

The launch of this publication coincides with the holding the United Nations Framework Convention on Climate Change's thirteenth Conference of Parties (COP-13) that will take place at Nusa Dua, in Bali, between December 3 and December 14, 2007. ITU will also be holding its Global Forum on Effective Use of Telecommunications/ICT for Disaster Management: Saving Lives, where we are launching the ITU flagship initiative, "ITU Framework for Cooperation in Emergencies (IFCE)" which seeks to address recent challenges in the area of emergency telecommunications. Whilst an attempt has been made to deal with all important aspects, this Compendium is by no means encyclopaedic. The aim has been to produce a user-friendly product that demystifies complex technical issues, is comprehensive and compact, and contains useful factual information that is concise and organized for easy access by those seeking quick reference.

It is my hope that this publication will add value to all those actively involved in humanitarian assistance and those interested in this subject because telecommunications remain the bloodstream to effective disaster mitigation and disaster relief.

Dr Hamadoun I. Touré

Secretary-General
International Telecommunication Union

SUMMARY

VOLUME I

ITU-D CONTRIBUTION

TO THE COMPENDIUM OF ITU'S WORK

ON EMERGENCY TELECOMMUNICATIONS

Table of Contents

Page

Page

Figures

Tables

PART I

CHAPTER 1

Telecommunications for disaster mitigation and relief

1 Introduction

Highlighting the role of telecommunications for humanitarian assistance, former United Nations Secretary-General Kofi Annan said:

> *Humanitarian work is one of the most important, but also one of the most difficult tasks of the United Nations. Human suffering cannot be measured in figures, and its dimensions often surpass our imagination, even at a time when news about natural and other disasters reaches every corner of the globe in next to real time. An appropriate response depends upon the timely availability of accurate data from the often remote and inaccessible sites of crises. From the mobilization of assistance to the logistics chain, which will carry assistance to the intended beneficiaries, reliable telecommunication links are indispensable (ICET-98).*

Telecommunications is critical at all phases of disaster management. Drawing from various sources that include telecommunications satellites, radar and telemetry, and meteorology, remote sensing for early warning is made possible. Before disasters strike, telecommunications can be used as a conduit for disseminating information on the impending danger thus making it possible for people to take the necessary precautions to mitigate the impact of these disasters. Recent statistics show that annually disasters are killing more than 25 thousand people, displacing more than a million, and causing economic losses of up to US$ 65 million.

When disaster eventually strikes, coordination of relief work by national entities, as well as the international community is made possible. Recent experiences have demonstrated this as the Telecommunication Development Bureau was called upon to deploy satellite communication equipment for both telemedicine and basic voice communications in the immediate aftermath of disasters in countries affected by the tsunami – Pakistan after a major earthquake, Suriname following floods, Peru after an earthquake, Bangladesh after devastating floods, and Uganda after huge floods that destroyed most of the basic infrastructure. Telecommunications also play a critical role in facilitating the reconstruction process and coordinating the effort of getting returnees displaced by disasters back to their original homes.

It is clear therefore that telecommunications play a pivotal role in disaster prevention, mitigation, and management. Other telecommunication applications ranging from remote sensing and global positioning systems (GPS) to the Internet and Global Mobile Personal Communications via Satellite (GMPCS), have a critical role to play in tracking approaching hazards, alerting authorities, warning affected populations, coordinating relief operations, assessing damages and mobilizing support for reconstruction.

1.1 The need for a Handbook on Emergency Telecommunications

Well-crafted handbooks provide invaluable reference materials to students, the newly qualified practitioner, the seasoned operative, the policy-maker, and any other person or organization with an interest in the field covered by that particular handbook. This handbook is no exception as it is written to serve as a close companion to those involved in the noble work of providing as well as using telecommunications for disaster mitigation and relief. It simplifies and demystifies the complex technical issues that characterize the fast evolving field of telecommunications especially in this era of convergence and emergence of next generation networks. For this reason, while this handbook is meant to be simple, it is comprehensive, compact and contains useful factual information that is concise and organized for easy access especially by practitioners.

Part I of the Handbook consists of three chapters including this first introduction chapter. Chapter 2 looks at the organizational framework of emergency telecommunications. It discusses disaster prevention, response, and the available means of telecommunications.

Part II has seven chapters focusing on the operational aspects of emergency telecommunications. Chapter 1 discusses telecommunications as tools for the providers of emergency response while Chapter 2 looks at public telecommunication networks and their role in disaster relief. Chapters 3, 4, 5, 6, and 7 look at the use of the Internet, private telecommunication services and networks, the amateur radio service, broadcasting, and emerging technologies respectively.

Part III discusses the technical elements of emergency telecommunications. This segment is critical especially for field practitioners who are often confronted by technical challenges while installing and using telecommunications equipment in the field.

1.2 Who should read this Handbook

The Emergency Telecommunications Handbook, which is Volume 1 in this Compendium on ITU’s work on Emergency Telecommunications, is written to be read, studied and understood by every person who has responsibilities connected with the planning, usage, evaluation, or survey of emergency telecommunications systems or their vulnerabilities. It can be read as a stand-alone text or be used in conjunction with formal training opportunities in the field. It is a project of the Telecommunication Development Sector (ITU-D) of the International Telecommunication Union. This is an updated version of the Handbook on Emergency Telecommunications that was published in 2005 and is more enriched as it is accompanied by Volumes 2 and 3, covering emergency telecommunications issues in the Radiocommunication Bureau and Telecommunication Standardization Bureau. This volume and the Compendium are being launched at the same time with the ITU-D Best Practice on Emergency Telecommunications, which contains invaluable information on designing National Telecommunications Plans.

CHAPTER 2

Organizational framework of emergency telecommunications

2 Introduction

The description of the organizational framework of emergency telecommunications requires the definition of the two words, emergency and telecommunication. By definition, an *emergency* is simply a situation requiring urgent response. Depending on the circumstances, initial response will be provided by whoever is present, using whatever means are available on site. Any other additional intervention deemed necessary can best be mobilized mainly through *telecommunications*.

An emergency situation might develop into a *disaster*, either due to its very nature, or as a consequence of insufficient response to the initial event. The magnitude of the event will require resource mobilization on a regional or even international scale; *communication* related to a disaster will however include activities well beyond an alert requesting emergency response, made through the normally available means of telecommunications.

Corresponding to the use of the four terms in recently developed documents and in the work of ITU Study Groups considering the subject matter, the present second edition of the handbook covers the use of telecommunications as the logistics of information exchange in emergency and disaster situations. It does not cover communications in the sense of content, and its scope is not limited to telecommunications in the strict sense of the word.

2.1 Prevention and preparedness

Prevention, the avoidance of hazards, is a primarily local task. Telecommunications have a key role in the distribution of respective knowledge and the creation of awareness. They are the vital tools for early warning. *Preparedness* to respond to emergencies is a task of institutional responders, commonly known as emergency services. Due to the character of such services, their telecommunication equipment and networks can be expected to be in a permanent state of readiness. Response to disasters, including relief operations following such events, is likely to involve institutional responders, typically national and international humanitarian organizations. Different from usually local emergency services, these responders need to be prepared to operate in unpredictable locations and under widely different conditions. Telecommunications under these circumstances are a great challenge.

2.2 Response

Appropriate response depends first of all on rapid and accurate information exchange. An increasing complexity of administrative structures and the distribution of responsibilities in the response among authorities goes parallel to an increasing number of available communication links. Public networks, such as the fixed line and mobile telephone system are the mainstay of first level alert.

With the involvement of partners from outside the immediate vicinity of an event, the responsibilities and thus the communication requirements shift to larger dimensions. Decision-making in such unpredictable operation conditions becomes a process involving a multitude of institutions. In these circumstances, private networks, such as dedicated radio networks including satellite links are needed to bridge information gaps and facilitate information exchange.

2.3 Typical scenarios

Among the oldest tools for an electronic “cry for help” were fire alarms. Pressing a button on a street corner would ring a bell at the fire brigade, providing information only about one fact: the emergence of an emergency in the vicinity of that alarm button.

This basic system developed into publicly accessible communication facilities allowing the exchange of information in two directions with increasing bandwidth and increasing information content. Over the years the tools available to the emergency services have improved both in terms of the services and applications they offer and in terms o diversity. It is for this last point that inter-operability becomes a key issue, and will be a main consideration in Part 2 of this handbook.

Today, international disaster response and relief operations following catastrophic events are no longer limited to natural disasters such as earthquakes, but extend to wars and post terrorist attack scenarios. Planning for reliable telecommunications is critical irrespective of the nature of a disaster because existing publicly accessible telecommunication networks might be disrupted by the event itself, or even get overloaded due to increased demand for service. Provision of timely and additional private networks might be hindered by regulatory restrictions if appropriate arrangements are not put in place well in advance to pave way for effective participation by the players involved in international response.

2.4 The partners in disaster response

Initial response to any disaster is the responsibility of the local community. National, regional, and international assistance are only mobilized when it is realized that the required assistance goes beyond the resources and capacities of the local response mechanisms. Involvement of entities outside a sovereign state’s borders is conducted on a “request-offer-acceptance” basis. In all cases, coordination with national authorities is paramount.

Operating under volatile and difficult conditions, many organizations providing humanitarian assistance rely on dependable telecommunication networks and systems to coordinate their operations.

2.5 National disaster management structures

The attribution of disaster-related functions differs from country to country. In most cases, it follows the country’s administrative structures, with a disaster coordinator for each district, state, county or similar geographical division. The “horizontal” cooperation among specialized services at each level is as essential as the vertical “lines of command”. For disaster telecommunications this requires established links between disaster coordinators and telecommunications authorities and service providers at each level.

This need for coordination throughout the national structures also applies to international humanitarian assistance. In the latter case, the national government is the primary counterpart of the foreign providers of assistance, but their operational activities must be fully integrated with those at various national levels. A “Disaster Management Team”, normally convened by the United Nations Resident Representative and consisting of all international organizations present in the affected country is established in the capital. Its counterpart is the entity or official designated as national disaster manager. At the local level, an on-site operational coordination centre (OSOCC), usually established by a United Nations Disaster Assessment and Coordination (UNDAC) team, ensures the integration of international assistance with the national and local partners at the site of the event. Reliable communications are paramount to the effective functioning of each of these mechanisms and for their coordinated interaction.

2.6 International disaster management structures

It is to some extent due to the availability of global real-time telecommunications, that response to emergencies and in particular to major disasters includes more and more international partners. Some of these are institutional bodies while others may be constituted ad-hoc in response to acute needs. All of them will however respond to what information is made available to them, and their response will be determined by the timeliness and reliability of this information.

2.6.1 United Nations entities

The United Nations system includes specialized agencies for the various aspects of humanitarian work, including disaster response. Their cooperation is ensured through the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), headed by the United Nations Emergency Relief Coordinator with offices in Geneva and New York, and with field offices in a number of countries. Using a permanent, 24 hours per day/365 days per year duty system, OCHA uses all available means of telecommunications to monitor events, and to immediately alert the international community to mobilize appropriate resources in cases where international assistance is likely to be required.

In addition to maintaining its own telecommunication networks, OCHA carries out the functions of the Operational Coordinator as mandated by the Tampere Convention [see Chapter 4]. The office regularly convenes the Working Group on Emergency Telecommunications (WGET), an open forum including all United Nations entities and numerous international and national, governmental and non-governmental organizations involved in disaster response as well as experts from the private sector and academia. In between the two annual plenary meetings, the WGET partners meet in *ad hoc* working groups on specific issues and maintain a continuous exchange of information through electronic means.

In the event of an emergency, OCHA dispatches United Nations Disaster Assessment and Coordination (UNDAC) teams to a country affected by a disaster. Such teams typically arrive at the site of the event within hours and support the national authorities in the coordination of international assistance.

In the affected countries, the various entities of the United Nations system work together in the Disaster Management Team (DMT). Such a team is convened by the Resident Coordinator, in most cases the Representative of the United Nations Development Programme (UNDP), which has offices in almost all member states of the United Nations. Depending on the nature of the emergency, the various agencies and institutions provide assistance in their specific field.

In addition to OCHA, the United Nations entities most commonly involved in disaster response include the World Food Programme (WFP) providing emergency food as well as logistics services for other relief goods, the Office of the United Nations High Commissioner for Refugees (UNHCR), providing shelter and related assistance for the affected population; the World Health Organization (WHO) and the United Nations Children’s Fund (UNICEF), providing health services in particular for the most vulnerable groups. Depending on the nature of assistance required, other agencies participate in their specific fields.

Throughout the monitoring, alert, mobilization and response process, telecommunications are of vital importance. All United Nations entities maintain common and own networks, and have the capacity to extent such networks in cases where other means of communication are affected by a disaster. The interaction of all networks is ensured through the mechanism of the WGET, and in the affected country a Telecommunications Coordination Officer (TCO) is responsible for the optimum use of all available networks.

2.6.2 The International Telecommunication Union (ITU)

The International Telecommunication Union was established last century as an impartial, international organization within which governments and the private sector could work together to coordinate the operation of telecommunication networks and services and advance the development of communications technology. Whilst the organization remains relatively unknown to the general public, ITU's work over more than one hundred years has helped create a global communications network, which now integrates a huge range of technologies, yet remains one of the most reliable man-made systems ever developed. The work makes tremendous contribution to disaster prevention, preparedness, and response.

As the use of telecommunication technology and radiocommunication-based systems spreads to encompass an ever-wider range of activities, the vital work carried out by ITU is taking on growing importance in the day-to-day lives of people all around the world.

The Union's standardization activities, which have already helped foster the growth of new technologies such as mobile telephony and the Internet, are now being put to use in defining the building blocks of the emerging global information infrastructure, and designing advanced multimedia systems which deftly handle a mix of voice, data, audio and video signals.

Meanwhile, ITU's continuing role in managing the radio-frequency spectrum ensures that radio-based systems like cellular phones and pagers, aircraft and maritime navigation systems, scientific research stations, satellite communication systems and radio and television broadcasting all continue to function smoothly and provide reliable wireless services to the world's inhabitants.

ITU's increasingly important role as a catalyst for forging development partnerships between government and private industry is helping bring about rapid improvements in telecommunication infrastructure in the world's under-developed economies.

Whether in telecommunication development, standards-setting or spectrum sharing, ITU's consensus-building approach helps governments and the telecommunication industry confront and deal with a broad range of issues which would be difficult to resolve bilaterally. This is critical especially in the area of disaster mitigation and relief.

Article 1, Section 2 of the ITU Constitution provides that ITU shall "promote the adoption of measures for ensuring the safety of life through the cooperation of telecommunication services".

This mandate has been further enhanced through resolutions and recommendations adopted by past and recent World Telecommunication Development Conferences and World Radiocommunication Conferences, and ITU's Plenipotentiary Conferences, as well as its active role in activities related to the Tampere Convention. The ITU works in close cooperation with the United Nations Emergency Coordinator and head of the Office of the Coordinator of Humanitarian Affairs (OCHA), and is a member of the Working Group on Emergency Telecommunications (WGET). The role of the Union under the Tampere Convention and related instruments is more specifically dealt with in Chapter 3.

2.6.3 The International Committee of the Red Cross (ICRC)

The ICRC has a specific status in international law, which distinguishes this body from non-governmental organizations (NGOs). While in many cases the ICRC is a provider of operational humanitarian assistance, its primary function is the implementation of the Geneva Conventions, which govern humanitarian law in cases of conflict. The ICRC delegations in many countries worldwide are linked by their own telecommunication network, which is reinforced as dictated by the magnitude of disasters.

2.6.4 International non-governmental organizations

International non-governmental organizations play a key role in the provision of operational assistance. A well-known example of an international NGO is the International Federation of Red Cross and Red Crescent Societies (IFRC) with its national member societies worldwide. The IFRC and other NGOs maintain their own telecommunication networks and support their national counterparts when normal channels of telecommunications are disrupted by a disaster. A new and important group among the NGOs, are commercial companies, such as Ericsson, who make available the expertise resources at their headquarters and their offices in many countries in support of disaster relief operations.

2.6.5 National governmental institutions providing international assistance

Similar to international organizations, national institutions in many countries provide disaster relief abroad. Examples are the Swedish Rescue Services Agency (SRSA), the Swiss Disaster Relief Unit (SDR), and the German "Technisches Hilfswerk". They often provide services in specific fields, providing their assistance under bi-lateral arrangements with the receiving country or act as implementing partners in United Nations relief operations. National organizations for international assistance usually provide telecommunications for their own needs, and often support other institutions, such as the United Nations, NGOs and national rescue services, with telecommunication support. National non-governmental organizations may in some cases assume similar roles to those of national governmental organizations.

2.7 Organizing emergency telecommunications

Real time information exchange is the backbone of all cooperation in emergency response, in preparedness and prevention, and in the assistance of those affected by disasters. The rapid technological developments and the numerous tools available, equipment and networks, have opened new possibilities. They can, however, not fulfil their task in the service of humanitarian work, if they are not fully integrated throughout the development and the implementation of operational concepts. Telecommunications are tools of an organizational structure, but they also need their own organisational support.

The availability and applicability of the most appropriate means of telecommunication in emergency situations is a result of close cooperation between those involved in humanitarian work, the manufacturers of equipment, and the service providers who run the various networks. This relationship will make objective assessments of what these technologies can and cannot do in various situations.

CHAPTER 3

The regulatory framework

3 Introduction

Maritime distress and safety communications have traditionally enjoyed privileges such as absolute priority and exemption from fees. The same rules apply for communications with and among aircraft. These privileges do not however apply to emergency telecommunications on land. Recognition for their applicability in emergency and disaster situations has been recognised only recently, but much still remains to be done.

Telecommunications have a dual character. While their control and regulation is considered as an element of sovereignty of each State, by their nature, they do not respect national borders. For this reason, international regulation is indispensable, and national regulation is left to deal with issues related to national interest. In the area of emergency telecommunications, this means that an international framework has to be established and that international legal instruments have to be created to provide guidance. At the same time, national legislation to safeguard national interests has to conform to enacted the applicable international law.

3.1 The creation of an international regulatory framework for emergency telecommunications

Effective and appropriate humanitarian assistance cannot be provided in the absence of functioning telecommunications. This is all the more important when there are many players on the ground be it before, during or after a disaster. Owing to this importance, various concerned parties involved in both disaster relief and mitigation as well as telecommunication development have over the years recognized the need for an international framework on the provision of telecommunication resources for disaster mitigation and relief operations. In 1991, an international Conference on Disaster Communications was convened in Tampere, Finland, and was attended by disaster and telecommunications experts. The Conference adopted the Tampere Declaration on Disaster Communications, a declaration of experts without the status of a legal document, stressing the need to create an international legal instrument on telecommunication provision for disaster mitigation and relief. The Conference recognized that regular communication links were often disrupted during disasters, and that regulatory barriers often crippled the use of emergency telecommunication equipment across national boundaries. The Declaration requested the United Nations Emergency Relief Coordinator to cooperate with the International Telecommunication Union (ITU) and other relevant organizations in solving this and other regulatory hurdles in support of the goals and objectives of the International Decade for Natural Disaster Reduction (IDNDR). It invited them to convene an intergovernmental conference for the adoption of a convention on disaster communications.

The Tampere Declaration was annexed to the unanimously adopted Resolution No. 7 (Disaster Communications) of the first World Telecommunication Development Conference (WTDC-94, Buenos Aires, 1994). This Resolution urged all administrations to remove national regulatory barriers in order to allow the unhindered use of telecommunications in disaster mitigation and relief. It also requested the Secretary-General of the ITU to work closely with the United Nations and within the framework of IDNDR towards an international convention on disaster communications.

A few months later, the ITU Plenipotentiary Conference (PP-94, Kyoto, 1994) endorsed the WTDC resolution by its Resolution No. 36 (Disaster Communications). This resolution reiterates the need for an International Convention on Disaster Communications, and reinforces WTDC-94 Resolution No. 7 in urging administrations to reduce and/or remove regulatory barriers to facilitate rapid deployment and effective use of telecommunication resources for disaster relief operations.

These resolutions were further reinforced by Resolution No. 34 and Recommendation No. 12 of the Istanbul World Telecommunication Development Conference of 2002 (WTDC-02) and Resolution No. 36 of the Marrakesh Plenipotentiary Conference of 2002 (PP-02). In 2006 the World Telecommunication Development Conference (WTDC-06) adopted Resolution 34 (Rev. Doha, 2006) on the role of telecommunications/information and communication technology in early warning and mitigation of disasters and humanitarian assistance, and an ITU-D Study Group 2 Question 22/2 on the utilization of ICT for disaster management, resources, and active and passive space-based sensing systems as they apply to disaster and emergency relief situations. Later that year, the ITU Plenipotentiary Conference that was held in Antalya (PP-06) adopted Resolution 36 (Rev. Antalya, 2006) on telecommunications/information and communication technology in the service of humanitarian assistance, and Resolution 136 (Antalya, 2006) on the use of telecommunications/information and communication technologies for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief.

Pursuant to these resolutions, and the mandate derived from the Inter Agency Standing Committee (IASC, the UN advisory body on humanitarian affairs), the Working Group on Emergency Telecommunications (WGET) was established. Since 1994 the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) and its predecessors, UNDRO and DHA, convene its meetings, which serve as an open forum for the discussion of all emergency telecommunication related issues. The WGET includes all partners in humanitarian assistance and emergency telecommunications. This includes United Nations entities as well as major international and national, governmental and non-governmental organizations, and is open to experts from the academia and the private sector. Among its basic tasks of coordination and standardization of information exchange in humanitarian assistance, the WGET developed and reviewed drafts of an International Convention on Emergency Telecommunications.

3.2 International regulatory instruments on emergency telecommunications

The ITU Secretary-General circulated a first official draft of the "Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations" to all ITU Member States in 1996. The World Radiocommunication Conference (WRC-97, Geneva, 1997) unanimously adopted Resolution No. 644, urging all administrations to give their full support to the adoption of the proposed convention and its national implementation.

In the same way, the second World Telecommunication Development Conference (WTDC-98, Valletta) adopted Resolution No. 19 that goes beyond the endorsement of all the aforementioned resolutions. It invites the UN Emergency Relief Coordinator and the WGET to collaborate closely with ITU in supporting administrations as well as international and regional telecommunication organizations in the implementation of the Convention. The ITU telecommunication Development Sector was invited to ensure that proper consideration given is to emergency telecommunications as an element of telecommunication development, including the encouragement for the use of decentralized means of telecommunications. This handbook is an example of the response by ITU.

International efforts in emergency telecommunications came into fruition when from 16 to 18 June 1998, at the invitation of the Government of Finland, 76 countries and various intergovernmental and non-governmental organizations participated in the Intergovernmental Conference on Emergency Telecommunications (ICET-98) at Tampere, Finland. On 18 June 1998, thirty-three of the participating States signed the treaty, now called the Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations.

In 1998, the ITU Plenipotentiary held in Minneapolis unanimously urged national administrations to sign and ratify the Tampere Convention as soon as practicable. Its resolution 36 also calls for a speedy application of the Convention. Furthermore, the 54th session of the United Nations General Assembly, 1999, in its Resolution 54/233 also called for the ratification and implementation of the Tampere Convention.

3.3 The Tampere Convention

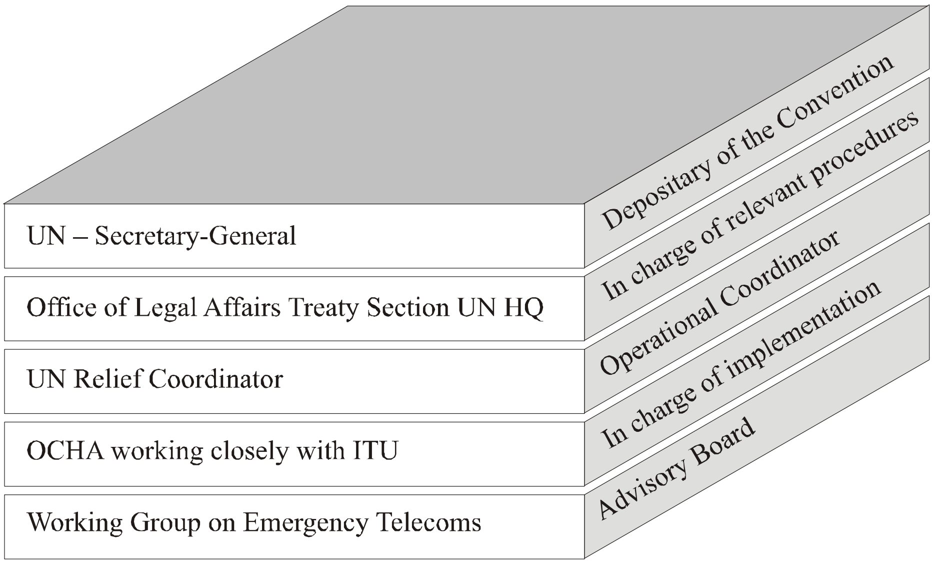
The structure of the Convention follows the format, which is characteristic of international treaties, and its text contains, in addition to the substantive paragraphs, the stipulations required in a treaty deposited with the United Nations Secretary-General:

- The Preamble of the Convention notes the essential role of telecommunications in humanitarian assistance and the need for its facilitation, and recalls related major legal instruments, such as various Resolutions of the United Nations and those of the International Telecommunications Union, which led to the birth of the Tampere Convention.
- Article 1 defines the terms used in the Convention. Of particular significance are the definitions of non-governmental organizations and non-State entities, as the Tampere Convention is the first treaty of its kind, which attributes privileges and immunities to their personnel.
- Article 2 describes the operational coordination, to be carried out by the United Nations Emergency Relief Coordinator.
- Article 3 defines the overall framework for the cooperation among States Parties and all partners in international humanitarian assistance, including non-State entities.
- Article 4 describes the procedures for request and provision of telecommunications assistance, specifically recognizing the right of a State Party to direct, control and coordinate assistance provided under this Convention within its territory.
- Article 5 defines the privileges, immunities and facilities to be provided by the Requesting State Party, again emphasizing that nothing in this Article shall prejudice rights and obligations pursuant to international agreements or international law.
- Articles 6, 7 and 8 define specific elements and aspects of the provision of telecommunications assistance, such as Termination of Assistance, Payment or Reimbursement of Costs or Fees, and establishment of a Telecommunications Assistance Inventory.
- Article 9 can be considered as the core element of the Tampere Convention, as the Removal of Regulatory Barriers has been the primary aim of the work towards this treaty since 1990.
- The remaining Articles, 10 to 17, contain the standard provisions concerning the relationship between the Convention's and other international agreements, as well as dispute settlement, entry into force, amendments, reservations, and denunciation. They state that the Secretary-General of the United Nations is the depositary of the Convention and that the Arabic, Chinese, English, French, Russian and Spanish texts of the Convention are equally authentic. These texts are available for free download at: www.reliefweb.int/telecoms/tampere/index.html.

3.3.1 Guidelines for the signature, ratification, acceptance, approval or accession

The "Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations" is an international treaty among States. It is binding for those States who have stated their accession to it, but all or part of its contents can at any time also be applied by reference in bi- or multi-lateral agreements governing international humanitarian assistance. The United Nations Secretary-General is the Depositary of the Convention (Art. 16). The Office of Legal Affairs, Treaty Section, United Nations Headquarters, New York, is in charge of the relevant procedures. The United Nations Emergency Relief Coordinator is the Operational Coordinator for the application of the Convention (Art. 2). The United Nations Office for the Coordination of Humanitarian Affairs (OCHA) is in charge of the implementation and execution of the respective functions and works closely with the International Telecommunication Union (ITU). The Working Group on Emergency Telecommunications (WGET) serves as an advisory board for this work. See Figure 1.

Figure 1 – Administrative parties involved in the Tampere Convention



A State may express its consent to be bound by the convention by:

- definitive signature;
- deposit of an instrument of ratification;
- during the intergovernmental conference (ICET-98) and for a limited period thereafter it was also possible signature subject to ratification, acceptance or approval followed by deposit of an instrument of ratification, acceptance or approval, such a provisional expression of consent is no longer possible.

The consent of a State to be bound may be expressed at any time; in view of the urgent need for the full application of the Convention it is, however, desirable, that the procedures for this purpose be completed with the depositary as soon as possible. Procedures relating to signature should follow the instructions in the attached note by the Legal Counsel of the United Nations. On all related matter it is advised that the assistance of the Treaty Section of the United Nations be sought. The Convention will enter into force thirty days after the deposit of such instruments by thirty States.

3.3.2 The main implications for states party to the Convention

Depending on applicable national legislation, the accession to an international treaty may require consultations with and/or approval by various legislative and executive bodies. The same applies to an adjustment of national laws, rules and regulations, which might be necessary to comply with the substantive articles of the treaty. In the course of these procedures the following aspects might deserve special consideration:

- The Convention has the purpose to expedite and facilitate the use of emergency telecommunications within the framework of international humanitarian assistance. Such telecommunication assistance can be provided as a direct assistance, provided to national institutions and/or a location or region affected by a disaster, and/or as part or in support of other disaster mitigation and relief activities.

- The Convention defines the status of the personnel of the various partners in international humanitarian assistance, including that of government entities, international organizations, non-governmental organizations and other non-state entities, and defines their privileges and immunities.

- The Convention fully protects the interests of the States requesting and receiving assistance. The host government retains the right to supervise the assistance.

- The Convention foresees the establishment of bilateral agreements between the provider(s) of assistance and the State requesting/receiving such assistance. Standard frameworks for such agreements will be developed by the WGET. To avoid delay in the delivery of assistance, “best practices” will be codified into common implementing language. The use of such model agreements, which will be made available in hard copy and electronic format, will allow the immediate application of the Tampere Convention in any sudden impact disaster.

The Convention came into effect on 8 January 2005. Currently, 36 countries have ratified the Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations. ITU-D has been providing assistance to ITU Member States on the ratification and implementation of this treaty. In 2007 events were held in Bandung, Indonesia for the Asia and Pacific region, Alexandria, Egypt for the Arab region, Yaoundé, Cameroon for the Central African Region, in Colombo, Sri Lanka, and in Male, Maldives.

3.4 Other international regulatory instruments and initiatives

The important role of emergency telecommunications has been recognized in a number of other Documents resulting from international Conferences and from the work of specialized meetings such as those of ITU Study Groups. In addition to the documents mentioned above in section 3.1 on the quest to create an international regulatory framework for emergency telecommunications, the following are some of the most recent documents seeking to reinforce these efforts:

- *Resolution 34 (Rev. Doha, 2006) of the World Telecommunication Development Conference WTDC-06 (Doha, 2006),* on “The role of telecommunications/information and communication technology in early warning and mitigation of disasters and humanitarian assistance” that instructs the Director of the Telecommunication Development Bureau to support administrations in their work towards the implementation of this resolution and of the Tampere Convention and invites administrations that have not yet ratified the Tampere Convention to take necessary action to do so as appropriate.

- *Resolution 36 of the ITU Plenipotentiary Conference (Antalya, 2006) on* "Telecommunication/information and communication technology in the service of humanitarian assistance" that invites Member States to work towards their accession to the Tampere Convention as a matter of priority, and urges Member States Party to the Tampere Convention to take all practical steps for the application of the Tampere Convention and to work closely with the operational coordinator as provided for therein.
- Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters adopted by the World Conference on Disaster Reduction organized by the United Nations International Strategy for Disaster Reduction (UN/ISDR) in 2005 [1].

3.5 Emergency telecommunications in the national regulatory framework

The implementation of international legal instruments may require changes to national laws and ordinances. In the case of the Tampere Convention, whilst the application of this convention concerns primarily telecommunication authorities, it also impacts a number of other government services such as those responsible for import, export and border control.

Advice and support on the creation of enabling telecommunication regulation and legislation in various countries for the successful implementation of the Tampere Convention can be obtained from the development arm of the ITU (ITU-D). This is in accordance with Article 12.2 of the Tampere Convention.

3.5.1 The development of a national disaster communications concept

As part of the implementation of the Tampere Convention, pilot projects will have to be carried out in several developing countries aimed at assessing the strengths, weaknesses, opportunities and threats of the existing disaster communications networks. These projects should attempt to study and evaluate background information on prevalent disasters in a country, the problems and constraints of disaster communications, the existing disaster-response operational structure and the equipment and personnel involved. Based on such information, recommendations – institutional, regulatory, technical and financial – will be presented for consideration by the appropriate national authorities as basis for improving or building a national disaster communications concept.

3.5.2 An overall concept

The specific situation in each country will have to determine the structure of the study. The WGET secretariat can assist in the identification of experts with experience in the assessment of national disaster communications structures and the development of concepts.

3.5.3 Methods and scope of a study

Studies of this nature require the full involvement of disaster managers and telecommunications entities if the studies are to achieve the set objectives. In these studies focus should be on all available communications networks i.e. public networks as well as private networks such as those run by public safety institutions, links to maritime and aeronautical networks, other specialized networks, and links to the Amateur Radio Service.

[1] The Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters could be downloaded from the UN/ISDR website at: www.unisdr.org/eng/hfa/hfa.htm

3.5.4 Confidentiality considerations

Experience shows that gathering information on network vulnerability may not be possible without the approval of senior management and governmental officials since the vulnerability of national telecommunication systems might be of great interest to would-be-saboteurs. For this reason, accurate information about the exact layout of networks may be hard to obtain as it might be considered classified as a strategic installation. In that case telecommunication staff may be reluctant to give information, when questions are asked for the purpose of disaster preparation and network operators may not give information unless they receive clearance from designated government officials.

Authority for a study of the vulnerability of systems will usually have to come from the highest levels of the authorities and entities concerned. A "Non Disclosure Agreement", "Non Disclosure Forum" or "Memorandum of Understanding" may be required before such clearance is given.

3.5.5 The need for a coordinated approach

Emergency preparedness is most effective when the responsibilities, resources and objectives of government and industry are merged through joint planning. Such planning fosters a sense of common purpose amongst separate jurisdictional authorities and results in a spirit of cooperation that arises during the planning process as well as in actual emergency situations. Furthermore, such cooperative and coordinated approaches provide a forum in which problems can be openly discussed, mutually acceptable solutions sought, and agreements reached. A typical of this is the successful creation of the Canadian National Emergency Telecommunication Committee (NETC) and of 10 Regional Emergency Planning Committees (RETC).

3.5.6 Telecommunications operators

In many countries de-regulation and privatization of telecommunications has taken place, resulting in competing operators. Information about the capacity of an operator's network may be of commercial interest to a competitor. This can result in reluctance on the part of operators to respond to questions. An instruction to release such information would have to come from the most senior level of management. Experience has shown that "Business Continuity Manager", often reporting directly to the Chief Executive Officer (CEO), are strategic persons to work with. Such an individual is best placed to know about the vulnerabilities of the existing system. Many companies have a "business continuity plan". Such a plan details the position of spares and the logistical plans for rapid restoration of services, and restoration of data.

3.5.7 Results

The results of the study, supplied by the network operator, may be difficult to interpret. It will likely refer to "Erlang" values and high-level PCM capacities but may avoid mention of transmission methods or back up power systems. Businessmen may tend to emphasize the strengths and play down the weaknesses of their networks, and an independent researcher will have to keep this in mind when performing the evaluation.

The study should consider three related but different issues:

- Capacity.
- Vulnerability.
- Rapid recovery.

3.5.8 Network capacity

Very few telecom systems are designed to carry all the traffic that the users could possibly generate. That would be hopelessly uneconomical, so the designers make various assumptions about what the highest load on a busy working day is likely to be.

A typical residential area switch design assumes that about 5% of the users will be using it at any one time. In business districts, this figure may be closer to 10%. For example, a typical 10 000 line exchange in a residential area may be able to carry only 500 phone calls at any given time. The 501st person to make a call will get a "congestion tone", or no "dial tone".

Traffic on any network still functional after a disaster, is likely to increase dramatically. It is therefore important to study how systems behave during acute overload situations. In some systems, a public switch will respond to an overload situation by sending a signal to surrounding switches advising them that the incoming routes to the switch are closed. In this case it will not be possible to reach any subscriber on that switch from outside, but it will still be possible for users of that switch to make calls to the outside. Planners should reflect this when designing information flows within their organizations.

Priority can be offered to some users of the network, but the details of how this is done and how priority users can be identified are potentially sensitive issues. In the case of "wireline" systems, it may be on the basis of prioritizing individual lines. In mobile systems, this may take the form of a "classmark" for the phone, or a "Preemptive capability indication" feature on the account, which allows certain users to jump the queue. In data systems it may take the form of differentiating the "sub-net" grade of service. In all cases where competition between operators exists, mandatory application of the same determination criteria for all providers of public network services is indispensable.

3.5.9 Additional vulnerabilities

The impact of natural disasters can further reduce the capacity of a telecommunications network by damaging elements on which it depends, such as power stations and the related distribution infrastructure, cable networks, switches and transmission stations. The resulting loss of power can be detrimental to a telecommunication system. Such damage will be discussed below.

3.5.10 Recovery

When equipment is damaged or destroyed, it must be replaced or repaired quickly. The operator will need rapid assistance from the supplier of the systems, who may be outside the country. The application of the Tampere Convention may help in this regard as it may facilitate the rapid passage of such equipment through customs authorities and may break whatever importation restrictions might have been imposed on a country by other State parties.

3.5.11 The implementation of the plan

A plan, which is developed in close cooperation with all those national entities that are concerned with disaster management or with telecommunications, has the best prospects of being fully implemented. Experience shows that the awareness for the need for any disaster plan is always highest in the aftermath of a disaster and diminishes quickly when time goes by without the occurrence of a major emergency. It is therefore essential to establish, as part of the plan itself, a mechanism for the periodic review of all measures taken in the implementation of a disaster communications plan.

3.6 The need for a common approach

Improvements to the regulatory environment for the optimum use of telecommunications in the service of response emergencies and disasters and of preparedness and prevention measures can only be achieved by joint efforts of all partners involved. It is the task of all national and international *providers of assistance*, to create the necessary awareness among the national regulators. It is the task of the *providers of telecommunication services and the suppliers of equipment*, to include provisions for the use of their goods and services in emergency telecommunications. It is the task of the *national taking part representatives* at Conferences run by international organizations to articulate the need for all entities to render support to all initiatives that favour the development, deployment and use of emergency telecommunications ITU forums provide the best opportunities.

A common and coordinated approach by all stakeholders results in a win-win outcome. The private sector that manufactures and provides the right equipment, creates a market for themselves and participate through their corporate responsibility; assistance provides benefit from efficient and appropriate telecommunications; the national authorities fulfil their role of ensuring a quality life for the citizenry, and those affected by disaster end up, being the ultimate beneficiaries as humanitarian assistance delivery will be facilitated by efficient information flow.

CHAPTER 4

Emergency telecommunications: Engendering prevention and response

When women and men confront routine or catastrophic disasters, their responses tend to mirror their status, role and position in society (DAW: 2001)

The importance of involving women in disaster preparedness and the promotion of gender sensitive responses invoke scepticism in the minds of many. This is partly because at the theoretical level the field offers little space for bringing in those issues that are directly related to women and men. Within this context, emergency telecommunications have been mainly defined as the challenge of establishing and maintaining the proper infrastructure. However all disasters are experienced locally by the children, women and men who live and work in the affected communities. Given this human dimension, approaches focused on the use of communications to facilitate disaster preparedness and response must substantively engage women as actors and not only as victims.

In most communities women perform the roles of key communicators and care givers. However, in disaster reduction activities they are most often marginalized. In general, reducing disaster risk involves effective preparedness, mitigation, response and recovery and is partly dependent on access to, and the appropriate use of, emergency telecommunications by vulnerable local communities and national and international institutions. A gender sensitive approach to effective and coherent disaster reduction accepts that those community members who are key communicators and care givers during normal weather conditions and peace time are also key actors before, during and after disasters. Given this reality, it is logical that they should be key participants in those training and capacity building activities that relate to reducing disaster risk.

Experience with both natural and man-made disasters highlight the simple truth that telecommunications are useful only to the extent that they are accessible to, and useable by, women and men in communities at risk. During disaster events many vulnerable communities are often cut off from national response systems due to a lack of appropriate telecommunications that should have been put in place before the disaster occurs. As disaster specialists note: while disaster telecommunications are used during the response and initial recovery (transition) phase, ***effectiveness is partially reflective of preparedness***. In this regard, training plays a critical role especially in the area of emergency telecommunications. As aptly noted in ITU's Handbook on Disaster Communications, "…training should be geared not only to those who are developing and implementing appropriate technologies and applications, but also […] to the users, to allow them to make the best use of what can be made available".

Decisions regarding who is trained in the use of telecommunications for disaster relief and recovery activities must however take into consideration the roles of both women and men. For example, an analysis of the 1991 cyclone in Bangladesh reveals that the largest number of casualties were women in part because their clothing prevented them from climbing to safer areas such as roof tops. In addition, because of the segregation between the sexes, many women did not receive the disaster warnings (South Pacific Disaster Reduction Program: 2002).

In identifying communities at risk it is also important to consider the make-up of households. In those low-income communities where there is a prevalence of female-headed households, women must be identified and targeted for training in disaster reduction activities, including in the use of emergency telecommunications equipment. Such training is critical because most often telecommunications used in disasters are focussed on providing information from the disaster site to relief and rescue agencies and vice versa in order to save lives and reduce suffering. Thus such training in the use of telecommunications also "serves the needs of the providers of assistance" (www.grameenphone.com).

Building on local solutions to redress gender inequality

Telecommunication is important before, during and after disasters because it enables government and international institutions to give warning of the impending disaster, to coordinate relief efforts and get information to those affected after disaster strikes. It is often the case that traditional telecommunication infrastructure is rendered inoperable after natural and man-made disasters. Further, many rural poor areas in developing countries already lack basic telecommunication infrastructure and do not have access to telecommunications to begin with.

Local programmes, such as the GrameenPhone in Bangladesh, can offer an effective, affordable and local solution to the telecommunication challenges experienced by relief organisations involved in disaster mitigation activities. The GrameenPhone program is implemented by Grameen Telecom (GTC) in cooperation with Grameen Bank, the micro-credit lender. This programme targets women from rural areas in Bangladesh. They are provided with the necessary financial resources to purchase a mobile phone which they in turn lease to other community members. This community mobile phone service enables female participants to both generate income and enhances their social status within their households and communities. GrameenPhone provides access to telecommunications by over "60 million people [... in] more than 68 000 villages in 61 districts" in Bangladesh.

(www.grameenphone.com).

Using appropriate technologies such as those based on satellite communications such local initiatives are particularly important when neither land lines nor terrestrial antennas are available to provide access to communication services, such as in disasters. Further, because women are the primary communicators in their households and communities and are often the ones to both heed warnings of disasters and plan for them, governments and disaster relief agencies stand to benefit from utilising such programmes in times of disaster and involve women who own and run them. Village phone systems such as the GrameenPhone can easily be transformed into an important element of the emergency telecommunications system. In so doing, more lives will be saved and economic losses reduced. This will also, acknowledge and empower women to actively participate in disaster response.

In identifying communities at risk it is also important to consider the make-up of households. In those low-income communities where there is a prevalence of female-headed households, women must be identified and targeted for training in disaster reduction activities, including in the use of emergency telecommunications equipment. Such training is critical because most often telecommunications used in disasters are focussed on providing information from the disaster site to relief and rescue agencies and vice versa in order to save lives and reduce suffering. Thus such training in the use of telecommunications also "serves the needs of the providers of assistance". (www/grameenphone.com)

Data on women as participants during disaster response is emerging. From available anecdotal information and case studies it is clear that women, because of their multiple roles within their households and communities, serve important functions before and after disasters, including the purchase of radios and batteries. Because they tend to avoid risk, women are more apt to heed warnings and prepare for disasters. At the local level they are active providers of assistance such as food. The Yokohama World Conference on Natural Disaster Reduction (1994) recognised this contribution from, and potential of, women.

Like age, being a man or a woman shapes an individual's lived experience. This is in part because the ways in which women and men navigate their communities as "women" and as "men" and their relations with institutions and with each other partly inform their experiences. In the context of disasters, though gender is not always or necessarily the defining factor in an individual's experience of, or response to catastrophe, it is a relevant dimension for both women and men. (Enarson, Elaine *et al.*: 2003). For example, men are more at risk of death during armed conflicts, while women are more open to listening to early warnings before a natural disaster strikes because they tend to be risk averse.

Our experiences of disasters increasingly confirm the critical role of emergency telecommunications before and after a disaster hits. Effective preparation for, and response to, disasters partially depend on the availability of communications as well as its use by those women and men of the community who are well placed to alert community members about emergency preparations, such as shelters, as well as inform them about available resources. Within this context the participation of women in emergency preparation and response is critical and their access to, and use of, emergency telecommunications are essential components in reducing risk.

PART II

CHAPTER 1

Telecommunications as tools for the providers of emergency response

1 Introduction

Telecommunications are indispensable tools for the operational emergency management. The speed of response and, most of all, the appropriateness of such response, depend on the real-time exchange of information among a multitude of partners. Reliable telecommunications are also a prerequisite for the safety and security of those who often risk their own life in their efforts to save lives and to alleviate the suffering caused by disasters. Last but not least, success in mobilizing of resources depends to a large degree on the quality of reporting from the site of an event.

To allow an effective and appropriate use of telecommunications in the service of emergency response, the users of telecommunications as well as the providers need to be aware of the particular operational aspects of emergency telecommunications. Disaster managers are often confronted with the task of defining requirements, and they can do so most realistically if they do not only know what is available, but are informed of what is feasible under given specific circumstances of an emergency situation.

Telecommunication service providers include enterprises providing services to the public or to specific users, mostly on a commercial basis, as well as those own telecommunication services established and run by emergency services and disaster response organizations. They also include the amateur radio service as a non-commercial resource provided by skilled volunteers. This segment of the handbook will look at two main elements. The first analyses the most common modes of telecommunications. The second looks at the networks and services using these various modes of telecommunications.

1.1 Interoperability and interworking

A major difficulty experienced by players involved in disaster management is the incompatibility of their telecommunication equipment and software. This problem has been experienced in almost all operations making the exchange of information difficult. This challenge is similar to that of military operations, that share with emergency operations a number of characteristics, such as a rapidly and often unpredictable changing physical and social environment, and the need for rapid and inter-dependent decision-making at all levels. Their telecommunication requirements are comparable. The military terms of tactical and strategic communications best describe what has to be provided for a coordinated response to any emergency having more than local implications.

In order to deal with this challenge, standardization of telecommunication networks is essential to achieve compatibility and make the exchange of information possible at least within the two groups i.e. technical and strategic networks. Sofar, gateways seem to be the only realistic solution although not an ideal one.

In tactical communications, this function is mostly carried out by a human interface – the operator or the disaster manager who uses more than one network at a time. For this, one needs solid knowledge of the structures and procedures of the networks involved. However, in strategic communications, automatic gateways that have been developed between different systems require the technical staff to be familiar with the technology and how it may be utilized.

1.2 Telecommunication modes

Practically all modes of communications on public and private networks have their role in emergency telecommunications. The following sections give an overview of available modes, which will be described in more detail in the technical annex to this handbook:

a) Voice

This is the most common and most suitable mode of communication for the real-time transmission of short messages and it has minimal equipment requirements. Its applications in disaster communications range from point-to-point wired field telephone links, VHF and UHF hand-held or mobile transceivers to satellite phones. It also includes public address systems and broadcasts via radio. Voice has as its major pitfall the lack of permanent record making the transmission and reception of complex information difficult. It however, remains, the only mode that does not require user interface making it the most personal mode of communications. In a critical situation this remains the most preferred mode.

b) Data links

Data links were in fact the earliest forms of electronic communication. The telegraph was in use long before the telephone, and wireless telegraphy preceded radiotelephony. It was, the development of electronic interfaces and peripheral equipment – replacing the human operator translating between Morse code and written text – which made data communications for many applications superior to voice. The first such interface with practical applications in disaster communications was the teleprinter or teletype machine, commonly known in commercial usage as “Telex”. Initially used on wired networks, it was soon on radio links. While very reliable and with a very low error rate on wired circuits, efficient use over radio required strong signals and interference-free channels. The requirement of considerable technical resources for a reliable radio teletype (RTTY) link limited their usefulness in emergency situations. Where national and at least parts of the international wired telex network are still maintained, they remain a potentially valuable asset for emergency telecommunications. Completely independent from the public telephone network, they are immune against any overload of the latter, and their robust technology increases the resistance against the physical impact of disasters.

c) Advance digital technology

Advanced digital technology allowed the development of new data communication modes, which eliminate the shortcomings of RTTY. The key to error-free links is the splitting of the messages into “packets”, and the automatic transmission of an acknowledgement of correct reception or a request for re-transmission. The earliest general application of automatic error correction is the ARQ concept, standing for “automatic repeat request”, with communication protocols known as TOR (Second-Generation Onion Protocol for asynchronous circuit), SITOR (Simplex Telex Over Radio designed to provide reliable RTTY communication under adverse conditions while maintaining an extremely low error-rate) and AMTOR (Amateur Teleprinting Over Radio which is a specialized form of RTTY). In ARQ (Automatic Repeat Query) mode, an automatic acknowledgement or request for re-transmission takes place after every third letter of the message. Different from RTTY, where the number of stations receiving a transmission is not limited, ARQ type signals can only be exchanged between two partners at any given time. To allow broadcasting, a somewhat less reliable version, “forward error correction (FEC) mode was introduced. In FEC, every “packet” of three letters is transmitted twice; the receiving station automatically compares the two transmissions and, if they differ, identifies the most likely correct content of the “packet”.

Further development led to even more efficient methods of data communications on both wired and radio links. The Internet as the most prominent tool for data communication has been dealt with in a more detailed way in a separate chapter. The Internet Protocol (IP) has also been adopted as the common standard of communications in dedicated radio networks of the major partners in international humanitarian assistance. The “Packet Radio” mode is most commonly used on VHF and UHF. Its derivative “Pactor” and various similar, often proprietary modes allow, through suitable gateways, the use of HF radio links for practically all functions of the Internet. Newer versions, such as “Pactor III” have further enhanced the speed and reliability of data communication.

d) Telefax

Telefax was the first mode allowing the transmission of images in graphic hard-copy format over wired and, to a limited extent, wireless networks. In its original form, fax images were carried as analogue signals over voice circuits such as the telephone network. The development in digital technology has led to new forms of image transfer, including the applications on the World Wide Web, and the use of fax mode has been greatly reduced.

e) Other advanced modes

Other advanced modes including those used for image transmission over broadband links, have provided new opportunities and have improved the provision of real-time information to many more publics beyond those in the fore-front of emergency responses such as the media. Their higher demand on bandwidth and on equipment tend to restrict their application in emergency situations.

CHAPTER 2

Public communication networks

2 Introduction

For the purpose of this Handbook on Emergency Telecommunications, a public network refers to that which ordinary citizens have access to. This is important to recognize because in the event of a disaster the public will tend to initiate calls to the country hit by a disaster and from that country to other countries where loved ones are located resulting in the overload of the telecommunications network.

Typically a public network is designed to allow about 5-10% of the subscribers to call and receive calls at the same time. However, in emergencies more people make calls and tend to talk longer resulting in jamming, blocking or congestion of the network. There are a number of measures that can be taken to deal with this challenge.

2.1 The Public Switched Telephone Network (PSTN, POTS)

The Public Switched Telephone Network (PSTN) is sometimes called the Plain Old Telephone System (POTS). This name gives the misleading impression that it provides only public telephone service. The global cable and switch network was, built to serve telephones. But in reality it carries nearly all telecommunication signals making the transmission of other applications and services possible e.g. Internet. Failure of the PSTN results in more losses than that of the telephone service. For this reason, those involved in emergency response must have a clear understanding of the operations of these networks and what can interfere with such networks functioning.

2.1.1 Local wireline distribution (twisted pair, last mile, local loop)

Unless one is using some kind of wireless system, voice and data transmission from a subscriber to the local exchange will be via a local cable.

In many places, telephone lines are open wires, or cables with numerous pairs of wires, suspended from poles. Such pole routes are themselves vulnerable to disasters involving high winds and earthquakes. Any disaster causing just one of the poles on the route to fall down, or the cable to be cut even at one point, will disrupt the circuit. Restoring service may take days especially if the roads are inaccessible. A move preferred approach is to have cables buried underground in ducts, thus reducing their vulnerability. Therefore, it is advisable to have all disaster management centres connected through underground cables as this significantly reduces the risk of loss of service.

The “local loop” used on the PSTN has the advantage that the telephone at the user’s premises is powered from a battery at the telephone exchange. If power at the user’s premises is lost, the phone will still work as long as the lines are not damaged. However, this does not apply to cordless phones, which will have a home base station powered by the domestic power. Every home and business should be urged to have at least one normal type phone i.e. one powered from its line.

In addition, many types of Private Branch Exchanges have a feature called “Fallback”. When the power fails or the system crashes, relays connect the incoming lines directly to certain fixed phones in the building. Management must know where these phones are and how they work then disseminate this information about how to use them after a power failure. It may however not be possible to have fallback if you have a digital link.

2.1.2 Wireless Local Loop (WLL)

Some operators offer access to their switches via “wireless local loop” (WLL) solutions. WLL relies on local Radio Base Stations (RBS). These provide a radio link to fixed radio units in the home, which in turn connect to telephones in the home or business. In some locations it provides lower cost and quicker installation than traditional wire line local loop.

One problem with WLL is that if the power in the user’s house is lost, the radio unit will be inoperable unless reliable alternative power is provided. The RBS stations do have backup power, but are connected to the switch via the local cable system. In other cases the base station is connected by dedicated microwave link. Nevertheless, wireless access may in some cases be less vulnerable to physical damage than pole routes, provided backup power is available.

“Private wires” used by enterprise systems are often routed through the local cable system of public networks. In such cases, damage to the latter is likely to affect any wire telecom system in the area i.e. public or private.

2.1.3 Switches (telephone exchange, central office)

Switches are the centre of a telephone system; they also present the most serious risk of failure during disasters because of their tendency to be overloaded. In a residential area, a switch is dimensioned to accommodate simultaneous calls by about 5% of the subscribers. In a business area this figure may be up to 10%. When the load is greater than what the switch is designed to handle, the switch gets “blocked”. It should be stated that the power system for the switch also supports the lines passing through for other purposes. Other things such as the Internet can fail if the switch fails because the multiplexers in the building and the repeaters down the lines are powered from the same exchange battery.

If the main power supply for the city has been cut off, the switches can be powered by diesel generators forming part or the switches. This diesel can last for few days. In recent Ice storms in North America, telephone service was lost due to shortage of diesel fuel for the switches. A good business continuity plan should be provided to prevent this, with emphasis the provision of adequate fuel and using the best the means to pump it.

It should be noted that switches can easily fail if the building housing them is destroyed.

Floods are also a cause for concern. Floods may cause the power system to fail at the switch due to short circuits. Where equipment has to be imported, restorations of services may take longer. Ideally switches should be sited in areas not prone to flooding or other damage.

Probable solution

Prioritization, whereby some users are given priority access to the available capacity over others, is one solution to the blocking problem. The technology to do this exists but work needs to be done on the regulatory side, to define i.e. to develop criteria of who has priority access over who. There is also the matter of indemnifying the networks against lawsuits from those who did not get access in their time of need. There are three basic strategies for prioritization. First, all access is blocked to everyone except certain privileged users. The problem with this is that it denies citizens access in time of real need. Second, priority users can jump the queue and be assigned the next free circuit. Thirdly, some users are removed from system in order to give others priority. The choice of strategy is the prerogative of the network operator and the regulator.

2.1.4 The trunk and signalling system (long distance system)

Trunk lines are links between switches; they carry calls on the long distance routes between cities. Trunks often carry hundreds or thousands of calls on one link, by a process called multiplexing. The links may be implemented by microwave radio, copper cables, or optical fibre, depending on the expected capacity of the link. The trend is now to use optical fibre systems. To reduce vulnerability, cables are often buried.

In developing countries, the most economical and popular way to carry trunks is by microwave relay stations. These are repeater stations, usually mounted on hills or high buildings. Microwave relay stations are however, often located in exposed locations, and may sometimes be in remote areas that difficult to access. Given the importance of these remote stations, state assistance in getting rapid access to these stations is strongly recommended.

Many modern trunk systems feature automatic recovery systems, such as Sonnet rings and other automatic re-configuration methods so that a redundant link or route can take the load from a failed link. This of course depends on quite a lot of redundant capacity being designed into the system in the first place. There are also cost considerations and in the present de-regulated environment mainly small operators in developing countries who have limited resources consider this a luxury.

Even in well developed countries there have been spectacular flops, caused by the gradual erosion of redundant capacity as it is sold to paying customers in today's highly competitive business. When the network rings are broken, there may not be enough spare capacity in the ring to carry the entire resulting load. For this reason, government may have to ensure that margins of redundancy are kept, in the national interest.

A special case is the "Signalling system No. 7" also known as the "CCITT 7" system. This is a special network which is used for switches to talk to each other, to help get the call set-up. It is however, not carried on a special network, but is often added to the normal links. The loss of the trunk network may also disturb the function of the SS7 system, causing general signalling problems in the network.

2.1.5 Integrated Services Digital Network (ISDN)

Integrated Services Digital Network (ISDN) is a circuit switched, transparent data service at high speeds, which can be increased in 64 kbit/s steps. A typical use is in video phones and in scientific and technical applications. Generally, the same switch carrying phone calls is also switching the ISDN, using the same trunking system. ISDN cannot therefore be described as being less or more reliable when compared to phone calls, because it shares the same equipment.

It does however have one significant advantage over the Internet. The Internet is a "best-effort-but-no-promises" kind of network, which will disappoint users during disasters because of loading issues that it will face. ISDN on the other hand guarantees that a certain bandwidth will definitely be available to the user while paying to keep the circuit open. It is therefore more reliable for such things as streaming video, audio or data provided that a circuit is set up.

2.1.6 Telex

The importance of Telex is diminishing as text messages are increasingly handled by e-mail. Nevertheless, Telex remains an important tool especially in developing countries. The Telex system consists of teleprinters or specially programmed computer terminals, connected to each other by means of the International Telex network. Telex messages consist of only upper case letters of the Roman alphabet and some punctuation symbols, using the Baudot code ITU-ITA2.

Telex has two distinct advantages over other systems. The most important one is that Telex is switched through a different switch to that used for telephone calls. This is important in the case of a disaster, because of considerations that the telephone switch is often overloaded. Telex exchanges are designed to handle high levels of traffic, and will not usually be overloaded by private calls.

2.1.7 Facsimile (Fax)

A facsimile machine (Fax) consists of a scanner, a computer, a modem and a printer in one unit. This combination allows the transmission and reception of pictures on a piece of paper.

You can use this to transmit hand sketched diagrams, messages in hand written script and photographs. A general weakness of fax is that it is usually carried over normal telephone circuits. It is therefore subject to all the shortcomings of the PSTN. Furthermore most fax machines depend on external power. They are also quite big and heavy and require a steady supply of paper, sometimes of a special type.

2.2 Mobile phones (cell phones, handie phones)

Mobile phone service is provided by a large network of ground based Radio Base Stations (RBS). Typically each one provides for at least 3 “Cells”. Software in the phone keeps the mobile station connected to the best cell for its current location.

When mobile systems are designed, they optimize two tings; coverage and capacity. Both of those factors affect how they behave in disasters. These factors affect analogue, digital and third generation systems in exactly the same way.

Radio Base Stations cost close to a quarter of a million USD each, and must have a payback period of up to 5 years. These are therefore often built in locations where there is enough traffic to justify them. The result is that, these are mostly built in urban areas and may be sparse in rural areas. As a result mobile communications for emergency response in remote and rural areas is often hampered.

In some countries differing operators won their license by different means. A “beauty contest” means that the operator needs to impress the regulator with his good quality of service, which often means good coverage. As a result he has a lot of loss making RBS stations which he must cross subsidise with his urban ones. This operator ends up with higher prices but better coverage in rural areas.

An “Auction” means that the company prepared to pay the highest amount for the license will get the license. Such an operator may not have to build loss-making rural stations and as a result with cheap prices in urban areas but with almost no coverage in remote areas. When responding to a disaster and one has to choose an operator, it is important to consider the issue of coverage more than that of cost.

Capacity means deciding how many traffic channels to assign to each station. There is a maximum capacity that each station can support, so when more capacity is needed, cells are split into small cells to support the required traffic. It is however not easy to increase traffic capacity, so mobile systems do suffer from congestion just as fixed line systems do.

In fact the situation is far worse for mobile systems because, the only traffic channels available to a particular mobile, are the ones it can “see” from its present position. Spare capacity on the other side of town is useless. Local congestion problems are a very serious weakness of cellular systems in any emergency case and so cellular should on no account be considered a primary communications mode for any disaster management purposes.

The RBS stations are connected to mobile switches by means of fixed lines or microwave links. If these fail then the station cannot work as a stand alone. They are also vulnerable to as they are over dependent on the PSTN network. RBS stations are powered by the ground mains power system. When the mains power fails they will only remain operational for as long as the batteries hold out, about i.e. 8 hours or so.

"Cells on Wheels" (COWs) are mobile base stations that can be taken to the scene and deployed to provide extra coverage or capacity. Networks should be encouraged to invest in them and deploy them as soon as a capacity problem is anticipated.

Mobile switches have limits to their capacity just as fixed line switches. The major problem with this technology is the constant blocking of base stations.

"Pre-emptive capability" is a feature of most mobile switches. Provided that you have "pre-emptive capability" on your account, someone else will be kicked off the cell to allow your call to go through. Needless to say it is quite hard to get yourself on the list. It may take government intervention to do so.

SMS and GPRS are methods that GSM uses to transmit text messages or other multimedia data such as e-mail. These methods don't use voice traffic channels to pass the message. They also have limited capacity. Since they are store-and-forward methods, the best solution is to slow them down rather than block them completely.

Cell broadcasting is a feature of many mobile systems. It transmits text in a downlink only stream, so that all mobiles in that cell can receive the text at the same time. Since it does not use a traffic channel, it is not prone to blocking, and is therefore very useful for mass messaging, for example for warning the public on a mass scale.

2.2.1 Pagers

Pagers can be characterized as a low speed narrow band, one way or two way radio communication system intended for the transmission of very short text messages. As a rule since the engineers have to budget for downlink coverage only, they can raise transmitter power as high as is needed, even hundreds of watts. Pagers often have very good "in building" penetration while mobile networks may not because of the need to budget for mobile access link budget. Paging stations typically date from the pre-cellular era. They are often housed on mountain tops in remote locations. They do however nearly always have back up diesel power and back up radio feed links. As a result they can be very reliable in times of crisis.

These days, more and more users are switching over to SMS because of its convenience. This has the advantage that loads on paging systems, have become thus avoiding the very low overload problem. Eventually pagers might be phased out as more and more companies that traditionally supported these services are getting out of this business. While pagers have been a preferred means of communications, the lack of a roaming facility has always been a disadvantage.

2.2.2 Business continuity planning

The role of private telecommunication operators in times of disaster remains a topical and debatable issue. Whilst these companies are in the business of making money, they too have a social responsibility to ensure that their networks supports efforts aimed at disaster mitigation and relief. These organizations should be made accountable by governments that should stipulate in issued licenses that each telecommunication company must have a business continuity plan and must observe international norms and standards of good practice in this regard.

2.3 Satellite terminals and satellite phones

Several systems, differing in their technological concept and their applications, are available for use in emergency operations. For the user, the difference is primarily in the size of the equipment and the coverage required.

2.3.1 Mobile terminals

The most widely used mobile satellite system at the time of writing is the Inmarsat system. Originally created under the auspices of the International Maritime Organization (IMO) in the early 1980s, to serve the international shipping community, Inmarsat is now a privatized enterprise offering service to maritime, aeronautical and land mobile customers.

The Inmarsat system consists of geostationary satellites. Mobile terminals communicating through Land Earth Stations (LES) handle traffic supported by PSTN and other public networks. Four satellites cover the surface of the earth with the exception of the Polar Regions. Part 3 of this handbook includes a map of the areas covered by the 4 satellites. LES are located in various countries, within the range of one or more satellites. The communication links consist of a connection between the user’s terminal and one satellite, a link from the satellite to an LES, and the connections from there into a terrestrial public network.

All Inmarsat terminals need to be set up so that their antenna can “see” the satellite covering the operational area. Most terminals have provisions to remotely locate the antenna outdoors, separate from the actual user equipment. Like all equipment using directional antennas, Inmarsat terminals cannot be used in a vehicle while in motion unless equipped with special antennas used primarily in the maritime service, compensating for the movement of the vessel or vehicle.

For use in emergency telecommunications, various types or Inmarsat “standards” are available and suitable:

- *Standard M and mini-M* are the most popular for highly mobile applications. Mini-M terminals are about the size and weight of a laptop computer, while Standard M terminals are the size of a briefcase. They enable connections with any PSTN subscriber world-wide, including other mobile satellite terminals. Most M and mini-M terminals have a port to provide connection to a Fax machine, and they also have an RS-232 data port for the relatively slow rate of 2.4 kbit/s. Subscribers can use this type of terminal for email by means of a Post Office Protocol (POP) connection. While Standard M terminals can operate anywhere within the coverage of the Inmarsat satellites, the use of mini-M terminals is limited to the coverage provided by spot beams of these satellites. Such spot beams, which allow the use of terminals with lower power and smaller antennas, cover most landmasses but not the oceans and many of the smaller or more isolated islands. The number of simultaneous connections any one spot beam can provide is however limited, and the use of a large number of users in one location might result in saturation of the spot beam covering the area concerned. Only a temporary re-alignment of spot beams can in some cases prevent this problem.

- *Standard C* is a store-and-forward text system, initially developed for maritime traffic and today is an integrated part of the Global Maritime Distress and Safety System (GMDSS). It transmits and receives e-mails as well as Telex messages. It is however not suitable for carrying large files of data, such as attachments. Standard C terminals are typically briefcase sized, but require peripheral equipment such as a laptop computer and a printer. Some service providers can also forward messages from Standard C terminals to Fax machines (but not in the opposite direction). Especially the new Mini-C *TT-3026L/M* is ideally suited for fleet management purposes (vehicle tracking) as well as for remote status monitoring/controlling (SCADA) applications. There is no voice capability on this very robust and highly reliable system.

- *Standard B* service offers ISDN Data at 64 kbit/s. Standard B equipment is considerably larger and heavier than Standard M terminals and intended primarily for stationary use, where it can provide connectivity for multiple, simultaneous users or high-speed data applications.
- *Standard A* was the first generation of Inmarsat mobile satellite terminals, offering voice, data and Telex connections. They operate in analogue mode, and are now obsolete. This version will most likely be phased out in the very near future.
- *Inmarsat GAN, also called M4 (TT-3080 and NERA World Communicator).* Effectively a much lighter and cheaper follow-on to the Standard B working on spot-beams. It offers 64 kbit/s Data, Packet Data Service (IPDS) which is comparable to GPRS, but with a much higher throughput, high quality audio for broadcasters, Fax with up to 14.4 kbit/s speed and low cost Mini-M quality voice. Available in portable, stationary and mobile versions with a tracking antenna.
- *Inmarsat Regional BGAN* also called *Satellite IP Modem. It has been in operation* since 2003 on leased capacity via the Thuraya satellite, and is useable only in the limited coverage area (footprint) of the Thuraya satellite. The term BGAN stands for Broadband Global Area Network working on the switched packet principle over a 144 kbit/s shared channel. The effective throughput does thus depend on the number of users in a specific area. The R-BGAN terminals are very light (1.6 kg) and measure only $24 \times 30 \times 4.3$ cm, thus ideally suited for quick deployment, fast file transfer purposes. The terminals come without handset as they are intended for data transfer only. Only the effectively sent/received Megabits are payable.
- *Inmarsat BGAN* is expected to become operational in 2005. This is a small light-weight satellite IP modem providing up to 432 kbit/s data throughput, to work via the new Inmarsat I4 satellites the first of which is scheduled to be launched in early 2005. According to Inmarsat the existing R-BGAN terminals will be upgradeable such that they can be used on the I4 satellites. The exact coverage area of this broadband switched packet system will be known only after the successful launch of the 3 planned I4 satellites.

2.3.2 Hand-held satellite telephones

Services of the Global Mobile Personal Communication Systems (GMPCS) allow the use of equipment very similar to terrestrial cellular telephones. They are particularly suitable for situations where a high degree of mobility is required, and while they still need a line-of-sight connection to the satellite or satellites, their mostly-omni directional antennas need not be aligned accurately. Different systems offer specific advantages but also have specific restrictions in respect to their applications in emergency telecommunications.

a) Thuraya

Thuraya is a system based on (presently) only one geostationary satellite having consequently a limited geographical coverage of about 100 countries. Its coverage spans Europe, North, Central Africa and parts of Southern Africa, the Middle East, Central and South Asia and the oceans in these regions. An extension of services, through the use of an additional geo-stationary satellite, is planned for 2005. The user equipment, similar to a cellular telephone, can be connected to auxiliary equipment such as a base station allowing the use of the handset indoors, while the antenna can be located outdoors. Where terrestrial GSM mobile phone coverage exists, the Thuraya phone can be set to automatically switch to this network. Thuraya phones report their position to the terrestrial gateway station; they do so using a built-in receiver for the Global Positioning System (GPS). They therefore require line-of-sight connection not only to the geostationary Thuraya satellite, but also to at least 3 of the orbiting satellites of the GPS system. The possibility of sending one’s GPS position as an SMS is a very useful feature, especially for humanitarian relief workers operating in dangerous areas.

b) Iridium

Iridium uses a constellation of 66 satellites in Low Earth Orbit (LEO) at only 780 km above the earth. The satellite covering the location of the user does not normally have a direct link to the ground station providing the connection into the terrestrial public networks, but connects to such a station through other satellites of the system. The LEO concept is similar to that of a cellular telephone system, the difference being that the cells (i.e. the satellites) move in 6 polar orbits, while the user remains stationary. The complexity of the system and necessary frequent handovers can affect the operation of the system. Iridium is a truly global system, its coverage also including both Polar Regions, which are out of reach for geostationary satellites. Whilst it is satisfactory for voice, it is not suited for data as the very frequent hand-overs from one satellite to the next do limit the achievable net data throughput to less than 2 400 bit/s.

c) Globalstar

Globalstar is a system that uses a constellation of 48 LEO satellites in 8 orbital planes with 6 satellites each, inclined at 52 degrees, flying at an altitude of 1 400 km thus covering an area from 70° North to 70° South. The actual coverage of the system is limited by the need for simultaneous direct connection to the user and a ground station or gateway within the coverage of the same satellite. From locations where no such simultaneous coverage exists, communication is not possible. The lack of gateway stations on the African continent makes Globalstar virtually unusable in Africa. Globalstar phones can work on terrestrial GSM networks where such coverage exists. Voice quality is excellent and the throughput in data mode is 9.6 kbit/s.

Most systems operate with billing procedures through SIM cards, allowing control and attribution of communication cost and international roaming on the GSM networks with which the service providers have respective agreements. Due to the relatively high tariffs, in particular for connections between satellite terminals of different systems, the public satellite networks are attractive only for the initial response phase, but they should not be used as primary means in longer-term operations.

Other systems offer regional coverage for example in North America (Motient) and Asia (AceS). Several concepts for global coverage in data modes including Internet access are in various stages of development or deployment. Such systems may in the future offer appropriate solutions for specific regions or requirements, and should be considered whenever national emergency telecommunications plans are being developed. They are however not suitable for international disaster response operations in unpredictable locations.

2.3.3 Direct video (and voice) broadcasting

Another low cost and practical method of gaining satellite connection is to use the services of the broadcast satellite. Typically in such schemes a circuit board is installed into a personal computer. Software then installs this as if it were an Internet service provider. The computer then gets fairly good speed Internet access over the satellite link, but at a much lower cost than with conventional VSAT. However the user is contending openly with other users at the same time, so there is no guarantee as to quality of service as there is with conventional VSAT.

Pros

- inexpensive,
- easy to ship,
- easy to set up, little ground work required for setting up,
- readily available from the shelf,
- quite OK and reliable for Internet browsing.

Cons

- Shared bandwidth,
- In complex emergencies when lots of other users deploy the same system even browsing becomes slow.

Problems with TCPIP e-mail exchange (like Notes replication). The priority on those systems is given to HTTP and during peak browsing hours (at the point where the beam lands) this almost wipes out the email replication. However during night time hours even the replication works quite well.

Pricing is significantly lower than with conventional VSAT, both in the capital costs of the equipment and in the monthly running costs.

Use has also been made of the downlink only data facility provided by world space radio's, Direct Voice Broadcasting. It has been used, for example to update intranet files that are small. Worldspace is DVoiceB. Typically it is used by FTPing daily update files of Intranet content to a Worldspace up-link site. WorldSpace then broadcast the file over its satellites to receivers in field offices. The receivers have a data adapter that feeds the bit steam to the USB port of a laptop running a client software. The laptop is effectively a single machine web server serving a mirror of the Intranet site.

There is no cost charged to the receiving partly, but there is a cost per megabyte charged for sending data.

The best configuration today is using a PCI card, to be installed in a Desktop PC, that has two receivers making it possible to receive both data and a voice simultaneously. This has very modest costs and could be compared to the costs associated with VHF radio.

CHAPTER 3

The Internet

3 Introduction

The Internet increasingly provides support for major operations and functions of organizations, including those with significant distances between headquarters and field offices. For governmental disaster workers, access to the Internet permits continuous updates of disaster information, accounts of human and material resources available for response, and state-of-the-art technical advice. As an important feature, messages can also be disseminated to groups of pre-selected recipients, thus allowing some form of targeted broadcasts.

The power of the Internet, specifically that of web-based information services, continues to grow and evolve. The integration of wireless (including satellite-based) technologies and of high-speed capability on wire connections will provide disaster managers with access to far more information resources than they are likely to use. In the context of disaster communications it is essential to always keep in mind that personnel at the site of an event has, first and foremost, the task to save lives. Specific information might greatly enhance the efficient and effective use of available resources, and disaster managers are managers, not reporters. On-site relief personnel cannot be expected to conduct information searches. They neither dispose of the time, nor, in most cases, of the peripheral equipment necessary to process such information in a format directly applicable to field operations. The same is valid for the provision of information from a disaster-affected location and the observations in respect to the use of facsimile and other graphic communication modes.

3.1 Applications

The use and application of the Internet to emergency telecommunications is unquestionable. The following are some of the ways that this technology can contribute in disaster relief:

- Sending and receiving email and using web-based directories to communicate with colleagues, suppliers, governmental and non-governmental organizations who can provide assistance.
- Tracking news and weather information from a variety of government, academic and commercial providers.
- Finding up-to-date geopolitical information, geographical maps, travel warnings, bulletins and situation reports for areas of interest.
- Accessing medical databases to gather information on everything from parasitic infestations to serious injuries.
- Participating in worldwide discussion lists to exchange lessons learned and coordinate activities.
- Reading and commenting on content at various governmental, and non-governmental websites to maintain an awareness of the large picture and how others are portraying the disaster.
- Registering refugees and displaced persons to facilitate reunification with relatives and friends.
- Reporting other than disaster related news, such as sports results, as a morale builder.

There are also certain disadvantages to an Internet-based information resource strategy. Generally, the web is associated with high bandwidth and costly connectivity. A lot more need to be stated concerning the web, for instance the need to maintain older legacy systems (non-Windows, non-high bandwidth connectivity) as a redundancy option in the event of a systems failure should always be considered. The fact that equipment is not of the latest technology does not mean that it has no use, and in critical situations the opposite may hold true. The high vulnerability of solid-state circuitry to static electricity and electromagnetic pulses has been overcome in some cases by the re-introduction of vacuum tube technology in critical applications Other important issues pertaining to the Internet-based information exchange are reviewed in the following section.

3.2 Privacy

The openness and global reach of the Internet – the same characteristics that make it attractive for users in a disaster situation – threaten the security of data transferred via the Internet. Some institutions use secure data networks that bypass the Internet entirely except as a last resort. Given the sensitivity of information especially in a complex emergency, data tampering may be an issue. The unsuspecting and sometimes accidental wide dissemination of debilitating computer viruses and spam could seriously affect computer systems at crucial points just when they are needed most.

Focus should not only be on sending messages on the net but on ensuring that security is assured. It is therefore necessary to employ secure technologies that are now readily available of the shelf in order to authenticate the source of the message. This includes the use of digital or electronic signatures created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. This form of signatures use what is known as "public key cryptography", which employs an algorithm using two different but mathematically related "keys", one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form.

3.3 Availability

There are limits to the robustness and flexibility of the network. As more and more important traffic migrates to the Internet, it becomes an attractive target for disruption by extremist groups. In addition to deliberate and malicious actions, denial of service can be a result of excessive demand. There have already been examples in the USA, where servers providing storm information from the National Hurricane Centre and the National Oceanographic and Atmospheric Administration were overwhelmed by demand during the approach of a storm. During a crisis, the most valuable information source will often be found to be the most difficult to reach.

3.4 Accuracy

The quality of information to be found on the Internet is probably no better or no worse than of information available through more traditional channels. The Internet decreases the time lag between events and the posting of information about them. This free market of information gives equal play time to valuable information as well as to material that is out of date, slanted, misleading, or just plain wrong. Therefore the user of information provided by Internet resources must in each case verify the source of information before forwarding or applying it.

3.5 Maintainability

One of the key paradigm shifts realized by the Internet is user-initiated, demand-driven access to information. While this change can increase the effectiveness of an organization and lower the costs of information dissemination, information needs to be processed. Web planners need to carefully define the scope of information to be hosted, verify its reliability, structure it in a logical way that allows easy access, and ensure continuous and prompt updating. The availability of the human resources for these tasks is as important as the acquisition of information itself.

CHAPTER 4

Private networks

4 Introduction

The term “private network” is used here to describe communications facilities available to specialized users like fire brigades, police, ambulances, utilities, emergency teams, civil protection, transport, government, ministries, and defence. These networks can also be used by business, corporate, and industry users. The network is usually owned by the private users themselves who can share it eventually in a multi – organizational environment. The users usually manage their private network, in some cases an operator can do it for his private customers.

These networks come in different forms. They can be wired or wireless, and they can share public networks resources, they can be fixed or offer mobility. These can be classified as:

- land mobile radio networks,
- maritime networks,
- aeronautical networks,
- enterprise networks,
- virtual private networks,
- location networks,
- satellite networks.

4.1 Land Mobile Radio (LMR) services

4.1.1 Land mobile networks

The access to private Land Mobile Radio networks (LMR) is reserved to closed group of mobile users who make short exchanges of voice and data of an operational nature during day-to-day, emergency and disaster situations for Public Protection and Disaster Relief (PPDR).

The communications can be duplex but can also be half duplex where one user can talk at a time by pressing a Push To Talk (PTT) button. The LMR networks differ from public telecommunication networks as they offer specific services like immediate call set up, group call, emergency call, priority call, end-to-end security, ambiance listening.

LMR networks offer very short call set up times, simultaneous voice and data, mobility, high robustness and ease of use in harsh urban, wide areas, mountainous environments. They can cover different sizes of coverage from one cell of a few metres to large countrywide areas and they can also be set up quickly if needed.

LMR is a family of standards and technologies which can be combined to offer the required voice and data service. This is due to the fact that emergency users have specific varying needs according to their role as civil protection, police, and emergency teams. For example the security level needed is different between users, the data rate of information is varied, and the type of terrain of the critical missions is different as it could be urban, country, or a hot spot.

LMR systems are categorized as narrow, wide and broadband according to the increasing width of their radio channel and to the data rate offered.

ITU-R report 8A/205 defines the radio communications objectives and requirements for Public Protection and Disaster Relief (PPDR). Three typical scenarios have been identified. These are day-to-day operations, (large) emergency, and public events, disasters. Typical applications (database access, messaging) are identified. Then, depending on the LMR system in use (narrow, wide and broadband) the possible applications are listed in order of importance depending on the scenario.

4.1.2 The different modes of operation

LMR systems offer six possible main modes of working:

- **Direct mode** where the communications are done directly between the terminals without using an infrastructure. This is very practical. It is like a walkie-talkie mode where every one in the range can listen to the conversations if they are on the same radio channel.
- **Network mode** where the communications are under the control of the LMR network infrastructure composed of Radio Base Stations and Switches.
- **Dual watch** where the terminal is in both direct mode and in network mode.
- **Repeater mode** meant to extend the coverage around a vehicle, or in a building.
- **Gateway mode** meant to connect two different incompatible systems.
- **Ad hoc mode** where the terminals themselves have an information routing role as there is no infrastructure.

4.1.3 The different main services offered

LMR systems offer a wide range of **teleservices** such as the following:

- Group calls allowing communication between a calling party and one or several called parties belonging to the same group. This is also called talk group.
- Emergency calls with automatic call set-up and pre-emptive calls.
- Broadcast call allowing one caller to transmit to multiple parties.

LMR systems offer a wide range of services:

- Security services such as: Authentication of the user, end-to-end encryption of the voice and data, protection against intrusion, and key management.
- Mobility services such as: Hand over, cell location registration, and presence check. The speed can be up to aircraft helicopter speed in order to allow air to ground communications.
- Voice Services such as: Access priority, discreet listening, preemptive priority, call authorized by dispatcher, presence check, call duration limitation, dynamic regrouping, and group merging.
- Data services such as: Access to a database, GPS support for location, short messaging, file transfer, and status transmission Video, and telemedicine can be supported if the data rate permits. Data rates offered by these systems vary between 2.4 kbit/s for short messages, images, and database query, to several Mbit/s for telemedicine, video, and file transfer.

LMR private networks serve emergency and disaster communications in two ways:

a) The regular users of the LMR network may be involved in disaster response activities. The different organizations may have different LMR systems and then they inter-work through gateways or through the emergency control centres.

b) The LMR network may be used temporarily as a back up to carry information from and to users who are not part of the mission critical user group.

The following sections look at the services that could be provided as part of emergency telecommunications within the context of the two options discussed above.

4.1.4 Technologies

This section will not cover the technical details of each listed system as they are described in ITU documents ITU-R report M.2014 dealing with technical and operational characteristics spectrum efficient digital dispatch systems for international and regional use, and ITU-R 8A/109E which the land mobile handbook on digital dispatch systems. Radio propagation is a complex process, but some principles are useful to know in order to understand the classification of related technologies and their evolution. Before discussing the various systems, a few key points deserve mentioning:

- Analogue radio technology is being replaced by digital technology which allows secure services, better spectrum efficiency, larger coverage, better quality of service, data transmission, duplex, and hand over.
- The larger the radio channel the more data it can transmit when needed by specific applications. A classification is done according to the size of the band. These bands could be defined as, narrow (for example 25 kHz channel width), wide (for example 300 kHz channel width) and broadband (for example 2 MHz channel width). The wider the band the higher the data rate.
- The higher the data rate the smaller the radio coverage.
- The higher the frequency the higher the penetration.
- Mobility makes transmission more difficult due to fading and change of radio cells while moving, this can introduce discontinuity in communication if no hand-over is performed.
- Antenna technology can boost range of the same radio technology.
- Modulation techniques can boost data rates for the same radio channel width.
- Increasing power transmission can increase the coverage.

Technologies under this theme can be classified as analogue or digital systems. Digital systems can further be classified on the basis of whether they are narrow band, wideband or broadband.

LMR systems initially use narrow band radio channels and may use trunking in order to share radio resources between multiple users in an optimized use of frequency. Wideband and broadband radio channels are generally used when higher data rates are needed for services such as file transfer, video, and telemedicine Analogue systems include the popular MPT1327. Below is a more detailed look at digital systems:

- ***Narrow band digital mobile systems***: TETRA, APCO 25, TETRAPOL and iDEN as listed and described in ITU-R document M.2014 and ITU-R 83/109E for LMR as well as DIMRS and IDRA. Other proprietary systems exist which are not standardized such as EDACS, FHMA. These systems are used in all types of terrain and coverage. They carry voice and data at rates up to 36 kbit/s.

- ***Wideband digital mobile systems*** are under development and are aimed at increasing the data rate. They are an evolution of the narrow band systems and are generally upward. Examples are: an evolution of the narrow band systems and are generally upward compatible. They are TAPS, TEDS in ETSI, APCO 34 and TETRAPOL in TIA. Some mobile public networks have developed a limited subset of LMR services like GSM/Pro and GSM R. Wideband is intended but not exclusively for urban areas where data traffic can be most critical. Data rates can go up to a few 100 kbit/s.
- ***Broadband digital mobile systems*** allowing very high data rates of a few megabits are under development for PPDR users and can be classified as follows: Body, Personal, Local, Metropolitan, and Wide Area Networks (BAN, PAN, LAN, MAN, WAN) depending on the coverage. Some technologies can already be used as WLAN – Wi-Fi but they still must be adapted to the users specific needs for example security concerns. It must be noted that these systems are mostly intended for hot spots emergency situations.

A subset of LMR services are offered on some public networks such as GSM, PSTN, and IP. The point to note here is that public networks are generally overloaded and end up being partially or completely destroyed in emergency and disaster situations. For this reason, these services are more appropriate for day-to-day operations and for some emergency situations.

These LMR technologies are robust against noise, and they offer the same coverage for voice and data irrespective of the type of terrain.

The equipment can be:

- Terminals such as portable handsets, mobiles, a data terminals.
- Radio base stations.
- Switches.
- Gateways to other networks.
- Repeaters.
- Emergency control centres.

All these can be fully included in self powered containers which can be carried either by air or by road to the emergency site.

The range of PPDR reserved frequencies used by the different systems varies according to countries and systems which makes inter-operability difficult. Work is however ongoing in ITU to have the same frequencies designated worldwide or at least per region, as defined in the World Radio Conference WRC-03.

4.1.5 Interoperability/Interworking

Often different organizations have different telecommunication systems yet they are expected to coordinate operations and talk to each other at the emergency – disaster site. They also are expected to communicate with other local or remote users.

In order for critical users involved in disaster operations to obtain inter-operability the following measures should be taken:

- Use of the same technology in the same frequency band so as to make roaming from one network to another possible using the same terminal.
- Use of the same equipment in direct mode on the same frequency.

- Use of multimode equipment handling different technologies in the same band. This is possible thanks to a new technology called Software Defined Radio (SDR).
- Use of multiband equipment in the same technology covering several radio frequency bands.

The mission critical users can inter work if:

- They can communicate through the emergency control centre of each mission critical users organization. Emergency operations are coordinated locally on the spot or remotely. This is done in the Emergency Control Centre which can be fixed or mobile, local or remote, in a vehicle, or in a shelter. The emergency control centre user can monitor the on the spot users, he may have information on a computer screen where he may view the location of the users and vehicles on maps in real time He can also communicate with the on site users or the remote users.
- They can use gateways which are intermediate equipment to interconnect different technologies LMR, satellite, GSM, public network.

It must be emphasized that in these situations of inter-operability and interworking, the services offered end-to-end can be a subset of those offered by the different networks separately. For example end-to-end security is no longer ensured if transcoding is needed at the gateway.

4.1.6 Wireless private area networks

Private area networks are just as can be noted from the name, private. These have a reserved licensed or un licensed frequency band for private use. These technologies have radio channels with a large frequency band of several MHz and belong to the broadband LMR family. There are different technologies offering different data rates, services, and distances of communication. The coverage depends on the type of antenna used, figures given for range, and frequency. Data rates are given only for indication.

Applications developed on top of the wireless private area networks standards allow the use of these private area networks for PPDR. They are classified according to their range as local, personal and body area networks.

Wireless Local Area Networks (WLAN)

WLAN are radio links allowing very high data rates exchanges (between 10 Mbits /s and 100 Mbit/s) in direct mode between equipment such as portable computers, but with no or very little mobility. This equipment can also work in an ad hoc mode. This technology uses for instance the 2.5 GHz unlicensed frequency range or 5 GHz range. This requires one to be careful due to Potential interferences as several other systems are in this unlicensed frequency range.

Wireless LAN standard IEEE 802.11 (also called Wi-Fi) has many versions named a, b, c, and d. One has to check compatibility between equipments versions and the security level offered by each version used. The range is around 100 metres depending on the environment, such as the obstacles like walls It is very sensitive and easily affected by terrain features.

The data rates depend on the number of users and can decrease rapidly. With an increase in the number of users. Data rate cannot be guaranteed when other applications are running. ETSI HIPERLAN2 is another standard converging to IEEE 802.11 which includes a high level of security and quality of service and hand over. However, mobility is very low.

Wireless Personal Area Networks (PAN)

PAN are used between pieces of equipment in close proximity like a portable computer, a PDA and a printer for example. Infra-red and bluetooth are examples of technology used. They allow short range data communications of a few metres, mainly for file access, file transfer, query. The frequency is in the range of 2.4 GHz and data rates are of a few 100 kbit/s. Mobility is not offered or very slow.

Wireless Body Area Networks (BAN)

BAN allow communications between different equipment that you wear on your clothes. Distances are very short and are around one metre, technologies like Ultra WideBand (UWB) are used. The frequency is in the range of 3.5-10 GHz and the data rates can go up to one Gbit/s.

UWB offers integrated 3D location service and suppers from slow mobility.

4.1.7 Coverage

These LMR technologies do not provide the same land size coverage. For example, a wireless LAN network allows only a few hundred metres coverage while penetration for radio is variable, and satellite radio is known to have a major drawback in not being able to provide coverage indoors. It must also be recalled that the higher the frequency band, the higher the possible data rate but the smaller the cell coverage.

Some systems can be configured from one cell to large national networks with many cells by adding a combination of switches, and of radio base stations. Repeaters are instrumental in extending the coverage area, while gateways make interconnection different telecommunication networks possible. It is also important to have some idea of the coverage size in order to avoid loss of communications.

As a general guideline, narrow band LMR technology offers coverage of one cell which is between 40 to 70 km in network mode, and a few kilometres in direct mode.

Wideband LMR technology can offer about the same coverage as narrow band using new antennas techniques such as MIMO. But generally speaking, coverage is smaller, and half the narrow band coverage. Broadband LMR offers smaller coverage, ranging from a few metres to a few kilometres.

In concluding this segment, it is fair to state that the figures given above are an estimate as coverage also depends on topographical factors.

4.2 Maritime Radio Service

The Maritime Radio Service uses frequencies on defined channels within the frequency bands allocated to this service. It is unlikely that a station of another service will need to communicate directly with a ship at sea, but the maritime radio service has, nevertheless, applications in disaster telecommunications. As its own emergency telecommunication system, the maritime service uses the Global Maritime Distress and Safety System (GMDSS). This service is only of use to ships and marine rescue centres for the purpose of safety of life at sea (SOLAS).

4.2.1 Maritime networks

For short-range communications, typically within 20 km, the VHF band is used. The standard distress urgency and safety frequency in the maritime VHF band is 156.8 MHz. By law, every ship is required to monitor this frequency 24 hours a day. In an emergency, it is recommended to first call the vessel on that frequency before moving to another channel to establish communication.

Ships may have an automatic selective call system called DSC (Digital Selective Calling), on VHF channel 70. To use this facility, the Maritime Mobile Service Indicator (MMSI) code of the ship is required. If this code is not known, the ship's name can be used in voice on VHF channel 16. In addition, coast stations must also have a MMSI. This code is assigned together with the station's call sign.

Another way to contact a ship if the MMSI code is not known is the use of an "all ships" code. This causes a text message to appear on the screens of communications terminals on board ships in range of the calling station. The originator will specify the desired ship, and both stations will switch to a voice channel.

While in port, a ship or boat may monitor a port operations channel. Once contact on a port frequency is established, the port radio station may assign a working channel.

A ship at sea may also be contacted through the shipping agent responsible for its cargo. This enterprise will be able to contact the shipping company operating the voyage, which will in turn have a reliable way of communication with the ship. The shipping line is likely to know the communications means available on board the specific vessel, and can assist with arrangements for direct contact.

4.2.2 Maritime public correspondence stations

Ships at sea maintain contact with the shipping line by means of satellite telephone services such as Inmarsat, or through coastal radio stations. If the vessel is equipped with a satellite Telex terminal, then it may be possible to communicate directly with the ship by Telex. Ships also often have an e-mail address, usually through a storage and forward system including a mailbox on shore.

On HF radio, many coast radio stations are set up for the purpose of public correspondence, offering phone patch service to PSTN phones. For long-range communications, HF radio frequencies are used.

Maritime coast stations traditionally accept disaster and emergency related traffic, even though the disaster relief station may be land rather than sea based. As with all radio systems, a license will be required from the country where the land station is operating. In an emergency situation, there has been flexibility on these issues, and a coast station might well accept to handle traffic from a station, which does not have an account with the respective service.

4.3 The Aeronautical Radio Service

The aeronautical Radio Service has frequency bands allocated for communication with and among aircraft, and additional bands are allocated for radio navigation equipment such as used during instrument flight. A station intending to communicate with aircraft in flight needs "air band" radio equipment. Land mobile service equipment is technically incompatible with that used in the aeronautical band; this is not only due to the different frequency allocations, but because the aeronautical service on VHF uses amplitude modulation (AM), whereas FM is the standard on VHF in the land mobile service.

4.3.1 Aeronautical networks

Civil aircraft are usually fitted with VHF radios operating between 118-136 MHz, using the AM modulation system. This is the standard for air to ground and air to air communication. In addition, some long-range aircraft, (but not all), may be fitted with HF radio equipment using the Upper Side Band (USB) modulation system. By far most communication is performed using a single frequency in Simplex mode, without repeaters. The heights of aircraft mean that they are easy to communicate with, even at very great ranges.

The international standard emergency frequency is 121.5 MHz AM. Many high-flying aircraft monitor this frequency when they are en route. This frequency is also monitored by satellites, which can determine the position of a radio calling on this frequency. For this reason, 121.5 MHz should only be used in the case of genuine life threatening emergencies. To contact an aircraft in flight without prior arrangement with the aircraft, calling on 121.5 MHz may get a reply, but this should be considered only as a last resort. Once contact has been made, both stations must immediately change to another working frequency.

Whenever possible, prior arrangements should be made when there is need to communicate with aircraft in flight. The local civil aviation authority should be asked for the allocation of a channel for such traffic, and respective information should be included in the agreement with the air carrier and in the briefings to the crew.

In disaster response operations, HF radio can play a key role in the airlift management. In such cases, the contract with the air carrier should specify that the aircraft is to be equipped for this type of communication. HF radios in the aeronautical service often feature a Selective Calling System (SELCAL). This works somewhat like a paging system and allows the crew to ignore calls not transmitted specifically to them. If a ground station does not have this capability, the flight crew needs to be instructed not to engage their SELCAL.

If no specific frequency for contact with disaster operations has been defined, 123.45 MHz is an option. Though not officially allocated to any purpose, it has come to be an unofficial “pilots’ chat frequency”. A pilot may not, however, be monitoring 121.5 MHz or 123.45 MHz, but rather a local or regional flight information frequency. Information about such channels can best be obtained from air traffic control centres in the region.

4.3.2 Aeronautical public correspondence stations

The aeronautical service includes public correspondence stations, similar to those of the marine radio station previously described. All over the world, HF radio stations are established for the purpose of relaying flight operational information between pilots and their bases, and to provide reports to the respective control authorities. In addition, however, they also make phone patches to landline telephones for personal calls, such as home to family members. This service is charged against a credit card or an account.

For disaster communications, aeronautical public correspondence stations can be contacted for phone patch traffic in the same way as maritime correspondence stations. To facilitate this, relief organizations may wish to open an account with such stations in advance and they will then also receive information such as a frequency guide. In all cases frequencies in use for flight operations are to be avoided by other as these are reserved for aeronautical users.

4.3.3 NOTAM

When filing a flight plan, pilots are provided with Notices to Airmen (NOTAM), safety related messages, referring to the path of their intended flight. Such notices include updates on the navigation and other relevant information provided in charts and manuals. In the case of major disaster response activities with involvement of air operations, details about air drop sites, temporary airstrips and related communications arrangements may be published in a NOTAM.

4.3.4 Private radio on-board-aircraft

Experience has shown that it is not a good solution to expect pilots to use a radio of the land mobile service. Land mobile FM radio equipment operates on other frequency bands other than aeronautical AM radio equipment, and additional equipment would have to be installed on board but this would be time consuming and would have implications with respect to air safety regulations.

A hand-held transceiver is hard to use in an aircraft, given the high noise levels in most light aircraft and even in some of the larger planes commonly used in airdrop operations. If such a link to the operations on the ground is inevitable, one crewmember should monitor this radio, independent of aeronautical radio traffic and use headphones. A skilled operator may then even succeed to get an extended range especially if the station is at a high making it possible to relay emergency traffic.

4.3.5 Special considerations involving communications with aircraft

A station of the land mobile service must never, even accidentally, give the impression that the operator is a qualified air traffic controller, as this might be misleading. A ground station which is not providing official air traffic control needs to make this fact clear at all times. Pilots must know when they are in uncontrolled airspace, and apply the respective rules.

Communication with aircraft should preferably be conducted with the captain, who may also be called the pilot in command. Only the captain is authorized to make decisions such as whether an aircraft will take off or land, and the captain’s decision can in no case be overruled.

4.4 Location services

Radio navigation systems have a complementary role in disaster communications. Hand-held equipment for personal use are available at low cost, and subscriptions or licenses are not required. The system most commonly used is the Global Positioning System (GPS), operated by the US Government. Available is also GLONASS, run by the Russian government, and an additional system, GALILEO, is being set up by Europe. GPS (and also the other mentioned systems) is using a set of satellites and ground stations. Some of the satellites must be in sight of the hand held in order to allow positioning. This is why this system works outdoor, and in open areas. There are however indoor systems such as UWB (Ultra WideBand) that can be used.

The above-mentioned systems provide global coverage, and commercially available hand-held receivers have a position accuracy of about 50 metres. Their indication of altitude above mean sea level is somewhat less accurate. For special applications, equipment with higher accuracy is available at higher cost. In many emergency applications, affordability and simplicity may well be more important than seeking to obtain the highest accuracy. In disaster situations, position finding serves three main purposes which are outlined below. Speed and time can be computed.

Humanitarian personnel in the field are exposed to high safety and security risks. The provision of reliable communication links in combination with position information is therefore vital. Assistance to personnel in danger includes two separate elements: search, and rescue.

The search is the more time consuming and often more costly part of such response, and if the distressed person is able to report his or her position, this will enhance the speed and appropriateness of the response. Location services will help facilitate the searching process.

4.4.1 Automatic vehicle location services

Periodic position reporting facilitates the provision of assistance and may at the same time provide essential information about potential hazards encountered by personnel at a disaster site. Positions can be read off from hand-held units in two ways, i.e. in coordinates, i.e. as latitude and longitude, or as a relative position. The use of coordinates requires that maps with respective grids be available, and that the operators be familiar with the use of the system. However, the exact locations on maps can be shown by using Global Information Systems (GIS).

Relative positions, the indication of direction and distance from or to pre-defined, fixed points, can be obtained from most hand-held GPS receivers. If an easily identifiable landmark is chosen as the reference point, this information can be more useful than coordinates, as it may be easier to interpret and even allows the use of a tourist or other less accurate map without coordinates.

Combinations of communications equipment and navigation systems, allow the automatic tracking of vehicles on a map displayed on a monitor screen in a dispatcher's office. Similar equipment in hand-held form is available for the tracking of individual users.

Logistics applications

Moving relief goods, supplies and equipment, is particularly difficult if drivers are not familiar with an area where road signs may not exist and language problems may furthermore hinder the acquisition of information. Knowing the coordinates of the destination, or its location in respect to a fixed reference point or landmark rather than just its name, can help to overcome these problems. Place names may be hard to write or pronounce, and are often duplicated within a close distance. Whenever possible, vehicles should be equipped with position locating equipment and drivers should receive training in its use.

Waypoints

Position finders may have a feature allowing the user to record his or her position. The unit will then allow the user to define this position as a waypoint. Storing such information along the route facilitates the return to any point passed previously. Others travelling the same route later can copy the waypoints to their equipment and follow the identified route. This will however require a systematic assignment of names to the waypoints.

4.4.2 Personal Locator Beacons (PLB)

A Personal Locator Beacon (PLB) is a body worn small radio transmitter designed to transmit positions, plus some information about the user, to a rescue centre. PLBs are intended primarily for the personal use by mountain climbers and yachtsmen. PLBs are more expensive than Emergency Location Transmitters (ELTs), but since ELTs are associated with aircraft and have limited accuracy, the PLB is recommended as personal equipment for field personnel.

When a specific button is pressed on the PLB, the position and the identity of the PLB is sent to the rescue centre via satellite. The voyage plan file is then associated with the PLB identity, and the contact details of the user's office can be recalled. The centre alerts the base of the PLB user or a rescue agency. It is the responsibility of the owner of the PLB to up-date the voyage plan regularly with the rescue centre. Such devices are valuable in cases of extreme isolation or when working in areas with high security risks.

4.5 Enterprise private services

Enterprise systems are small-scale systems intended for use by businesses and organizations. Except for their small size, their structures are similar to those of the corresponding public systems to which they are inter connected through gateways. They can be wired or wireless.

Larger institutions often maintain their own enterprise systems over wide areas which can be trans-national, between several sites.

In case of disaster, companies need to be able to be back to business quickly. Backing up their responsibility but they quickly must restore telecommunications to be able to get back into business. They need to reconnect to the back up information systems, and need to be able to allow remote workers to run their business again.

4.5.1 The Private Branch Exchange (PBX)

This is one typical example of an enterprise system. It consists of a telephone switch on the owner's premises, usually connected to PSTN lines. Internal cabling connects the switch to extensions throughout the premises. Connections among the extensions of the PBX are therefore independent of any external network infrastructures.

Connection to the public networks and Internet is ensured by gateways.

Today, IPBX technology allows the use of IP and Voice over IP (VoIP) where the PABX is a software based technology running on Personal Computers acting as multimedia terminals and can be inter-connected by wire or wireless. Voice and data run on IP.

Mobility in the enterprise can be added with wireless technologies like WLAN Wi-Fi and /or the Digital Enhanced Cordless Telephones (DECT).

The CENTREX service is a PABX function offered by the public network itself, it then is vulnerable to disasters.

The Intranet is the own internal Internet of the company accessible by the internal wired or wireless multimedia personal computers. It may be connected to the outside through firewalls and can be accessed securely remotely by:

- **SOHO** which is the small office-home office using the Internet services through Virtual Private Networks (VPN).
- **ROBO** which is the remote office-branch office using the VPNs.

The Direct Dial-In (DDI) systems commonly used today reduce the need for switchboard operators by associating each extension with an external number. Thus, a caller from outside may be unaware that the called party is on an extension. At the same time, however, the functioning of the PBX even for internal connections may be affected by a disruption of the public network.

One significant advantage of PBX systems is that the owners keep control of the quality of service. Since they are paying for the capacity of the switch, they can decide to allow for the much greater traffic that a disaster can generate. Since their circuits will not be allocated for public use, they will not be contending for capacity.

A PBX will only work if it has power. Generally, switches have battery backup power for a few hours. If the regular power remains disrupted for a longer period, a back-up generator will be required. A PBX may take some time to reboot after power disruptions.

If a PBX becomes inoperable due to a power failure, a “fallback service” comes into play. With this system, certain pre-defined extensions are connected directly to incoming lines. In fallback mode, only these fallback phones will work, while all others will be inoperable. Permanent private links to other parts of the organization do not necessarily ensure immunity from failures by the public system. If any part of the public system is affected by a switch power failure, private lines may be disrupted as well. Connection by direct cable-connection, that does pass through elements of other networks, may overcome this problem.

A common solution to improve disaster resistance is to use microwave links and satellite links for longer distances. Microwave link systems should be considered if there is line-of-sight connection between premises.

4.6 Unlicensed Local And Wide Area Networks

Unlicensed networks are often used in case of emergency and disaster as they are private networks often separated from the public networks.

4.6.1 (Virtual) private networks

Many medium and large organizations operate their own network interconnecting computers for electronic mail service, data base accesses, and intranet. The servers of the company are connected to the office computers by means of a Local Area Network (LAN), which in some cases may cover various premises of an enterprise. Such an arrangement is known as a Wide Area Network (WAN).

The links can be wired or wireless locally or remotely.

Wired VPNs

LANs and WANs have switches called “routers”. Their function is to send traffic not intended for a local server over a long-range link to another router on different premises. A router can have more than one link to more than one off-site router. This adds redundancy, as alternative links may replace disrupted connections.

Business users may be located remotely at home or in agencies which have to be connected securely to the company servers remotely.

VPNs are Virtual Private Networks set up on public networks offering a secured remote access. They allow private users to share public networks securely between them. Specific functions are needed on the public network to handle security and at the company premises to provide firewalls. Specific software is added at the remote end terminal in order to do a “secured tunnel” for communications end-to-end. In case of disaster they allow the user to work remotely and securely from home for example if offices are destroyed.

Wireless VPNs

Different solutions are operational which are replacing the wired solutions:

- DECT is a Digital Enhanced Cordless Telecommunication standard and wireless technology for corporate, business and commercial private communications. It replaces wired private telephones by cordless handsets and is unlicensed. Slow mobility is available. It is mainly used for voice but it can handle data. Security could be provided through encryption.

- Wi-Fi (IEEE 802.11) and WiMAX (IEEE 802.16) can respectively be used for short range and wide range broadband communications. ETSI HIPERMAN (these are <IIGHZ carriers, don't need line of sight, up to 15 miles range) and HIPER ACCESS (> IIGHZ carriers, needs line of sight connections, up to 5 miles range) can also be used.

4.7 Satellite Very Small Aperture Terminal (VSAT)

One way to improve the chances that an enterprise system will remain operational during a disaster, is to connect via satellite. This will make it free from both a failure by terrestrial infrastructure and congestion of the PSTN.

The acronym VSAT stands for "very small aperture terminals". The antennas determining the aperture typically range in size from less than one metre to 5 metres, depending on the frequency band used. They are mostly designed for fixed installation, but so-called "flyaway" systems are available for disaster recovery purposes. Further developments are expected to enhance their applications in disaster communications.

In general, subscribing to a VSAT service means the purchase of a group of channels for a fixed period. No other user will be sharing these channels, and the subscriber is guaranteed the use of these channels even when systems such as PSTN and mobile satellite are congested. This is a preferred alternative, but the cost is high and it may be economical only as part of a larger enterprise system. VSAT service is available from a number of commercial operators offering global or regional coverage. Services offered cover voice calls, fax, Internet access, and VPNs.

Alternatively, a demand assigned multiple access system (DAMA) can be used in case it should not be desirable to use a regular VSAT service as part of an enterprise system. DAMA permits access to bandwidth on a demand basis. The cost is likely to be lower, but there is a risk of not getting service when the demand on capacity is high.

If one is serious about reliable long-range communications, VSAT is a superior system. The terminal equipment must be protected from physical damage. The dish in particular should be placed where it is not exposed to flying debris during storms, while still maintaining its aim at the satellite. Following a storm or an earthquake an adjustment of the position of the antenna may be necessary, and special equipment in addition to the actual VSAT terminal is required for this.

VSAT systems connect the PBX directly at each end (location) by satellite link. This means immunity from failure by the ground services, as long as the earth station remains operational and has independent power. However, both the capital cost of the equipment and air-time charges requires serious consideration before a commitment is made. Another strategy is to use either satellite mobile phones, or fixed cellular terminals, as one of the outside lines. The terminal must have a standard 2-wire POTS interface in order to do this. When the terrestrial lines fail, the satphone can be used to initiate and receive calls.

Some institutions use private data networks for workstations. This is done to enable users to share file servers and printers. By far the most useful service provided is electronic mail (e-mail). A short-range system covering one building is called a Local Area Network (LAN). A network connecting different premises of the same institution is usually called a Wide Area Network (WAN).

4.8 Emerging technologies and trends

Technology is evolving very fast and emerging technologies are mainly in two main areas: the core network and the access network including inter-operability. Internet Protocol IP technology is being generalised in the core networks and data rates on the air are increasing to allow new applications like multimedia, video, and telemedicine.

The main ongoing developments are for services related to:

- Mobility
- Security
- Quality of Service (QoS)
- Inter-operability
- Data
- Voice, image and video coding

– ***Mobility*** is a major user requirement at high speed, allowing roaming from one network to another of different technologies. For example, if the user is under a LMR narrow band network with urban coverage and he moves out to a satellite wide area coverage and then to an in-building WLAN network, he wants continuity of service without any specific action by him. Hand over to maintain the communication is a necessity. These features are studied in large worldwide organisations such as the WWRF (World Wide Research Forum).

– ***Security*** is also an increasing user requirement in order to identify the user, to secure the information end-to-end. For example, IP develops a version called IP V6 which integrates security protocols. End-to-end security over heterogeneous networks is being developed under Secure Communication Interoperability Protocol (SCIP).

– ***Services*** offered to the user tend to become independent of the technology used, and will be seen by the user as similar whatever the standard is in use. The reason is that for private services, standards for access are many in both wireless and wired form and there is no convergence towards one unique access standard.

– ***Quality of Service*** is a difficult issue with priority schemes, and real time data. The core network tends to be IP based where Voice is transmitted over IP (VoIP) requiring specific Quality of Service (QoS).

– ***Inter-operability*** is a key objective, allowing roaming, (service) portability, priority schemes, end-to-end security, guaranteed QoS. The Next Generation Network (NGN) developments in ITU will address this issue.

Software Defined Radio (SDR) developments intend to allow multi-mode terminals to be able to handle different radio standards seamlessly.

– ***Data*** rates will increase with new wireless standards:

  • ***Wideband*** is being developed for the four narrow band systems referred in ITU:

    a) TETRA develops two wideband ETSI standards called TAPS and TEDS. TAPS is an evolution of 3GPP/3GPP$_2$, Enhanced Data Rates for GSM Evolution (EDGE), GPRS (General Packet Radio Service) and is for data only. TEDS is an evolution of TETRA narrow band for voice and data while APCO25 and TETRAPOL develop new wideband solutions in TIA TR8.

  • ***Broadband*** is being developed in several projects:

    a) The partnership project ETSI, TIA, MESA (Mobility for Emergency and Safety Applications) develops a "system of systems" for hotspot where the network is ad hoc (all nodes are mobile) and several communication protocols are involved. It will review the broadband air interfaces in order to select and get the adaptations of the existing ones to the private users' needs. Eventually it will develop a specific one.

    b) The IEEE 802.16 (WiMAX) and IEEE 802.20 Mobile Broadband Wireless Access (MBWA) specify (mobile) broadband wireless access for large coverage.

    c) The Ultra Wideband (UWB) forum specifies the air interface evolutions including 3D position location.

Voice coding technologies evolve to transmit better quality voice in smaller data rates and compression video algorithms also evolve to require smaller data rates.

Public networks implement some of the emergency telecommunications which will then be available and can be used in emergency situations:

• EMTEL is the emergency telecommunications project in ETSI which defines the emergency call with location (E112), and standardizes the interfaces between authorities and citizens, between authorities themselves, and between Public Safety Access Points (PSAPs).

• Public Protection and Disaster Relief (PPDR) in ITU develops the International Emergency Preference Scheme (IEPS), as dealt with in ITU-T Recommendation E. 107.

• Internet Emergency Preparedness (IEPREP) in IETF develops the Internet emergency preparedness to implement the priority scheme.

• 3GPP develops the Priority Access Service (PAS) in order to allow to implement priority, authentication features on the air. Fast call set up and group call will also be implemented.

• GETS (Government Emergency Telecommunications Service) group develops the authentication and priority scheme for wired links.

It must be noted that:

a) **PABX** functions are implemented more and more in the public network called CENTREX (CENTRAL Exchange) and become full IP solutions for voice and data.

b) **Satellite** networks like IRRIDIUM and GLOBALSTAR implement mobile solutions with a whole range of satellites which can be used also for emergency telecommunications.

CHAPTER 5

The Amateur Radio Service

5 Introduction

Among the radio services defined in the Radio Regulations (RR), and regulated by this international treaty governing all aspects of radio communication, the Amateur Radio Service (RR S1.56, Geneva 1998) is the most flexible one. Using modes from Morse code and voice to television and to most advanced data modes, communicating in allocated frequency bands ranging from 136 kHz (longwave) throughout the HF (shortwave), VHF and UHF all the way into the GHz range, amateur radio was throughout its history and still is today at the forefront of technology. Amateur radio operators form a global (long range) network, but they are equally at home when it comes to local (short range) or even satellite communications. Most of all, however, they acquire their skills because of their personal interest in the subject of radio communications, and they are the experts in achieving extraordinary results with whatever limited resources available.

These characteristics make the Amateur Radio Service a unique asset for communications under the often extreme conditions encountered in emergency and disaster response. Its technical information and training material covers the most critical aspects of emergency telecommunications and much of part 3, the technical annex of this handbook, is based on the experience gained during more than 90 years of public service communications. The operational characteristics of many elements of emergency radio telecommunications are best explained on the example of the amateur radio service. Most of the content of Chapter 5 is thus applicable to all radio communication services utilized in response to emergencies and disasters.

The amateur radio service should not be confused with “citizens band” or “personal radio” operations, which are forms of public networks and described in Chapter 2 of Part 2 of this handbook. Amateur radio operators have to pass an examination given by or on behalf of the respective national administration prior to the issuance of an individual, personal operator’s license.

The *International Amateur Radio Union (IARU)* is the federation of the national amateur radio associations existing in most countries. It represents the interests of the amateur radio service in the International Telecommunication Union (ITU) and in international conferences. IARU supports emergency telecommunication applications of its members and ensures the exchange of information and experience among them.

5.1 The roles of the Amateur Radio Service in emergency telecommunications

Its wide scope of activities and of the skills of amateur radio operators make the amateur radio service a valuable asset in practically all sectors of emergency telecommunications. The following few points characterize this service:

- It has a large number of operational amateur radio stations in all regions and almost all countries of the world, providing a network which is independent from any other. It has in many cases provided the first and often for a long time only link with areas affected by disaster. Examples for this go back to the early days of radio, but are also found in most recent events, such as the role played when hurricanes hit on islands in the Caribbean in 2004.

- Their skills make amateur radio operators a prime human resource for emergency telecommunications. Many operators apply their skills and experience in the service of humanitarian assistance, be it temporarily as volunteers with governmental or non-governmental organizations, or as emergency telecommunication professionals with units of international organizations and other disaster response institutions.
- The training programmes and emergency simulation exercises developed by some of the national amateur radio societies are applicable to all sectors of emergency telecommunications and can be adapted for training of all potential users of telecommunication in emergency situations.
- The technical documentation, literature and electronic resources, available for the amateur radio service, are unique resources for information on how to solve problems with often very limited and possibly improvised means.

The importance of the amateur radio service in emergency telecommunications has been recognized in many documents and was reconfirmed by the World Radiocommunication Conference WRC-2003 (Geneva, 2003), which modified article 25 of the Radio Regulations, facilitating emergency operations of amateur radio stations and related training of operators, and encouraging all States, to reflect these changes in their national regulations.

5.2 Amateur radio networks and their ranges

Three types of radio networks are typical for the amateur radio services, and all three are encountered in major disaster response operations.

5.2.1 Short-range networks

Typically provide operational or tactical communications at the site of a disaster and with the surrounding areas. They can include fixed, mobile and portable equipment and are mostly using frequencies in the VHF and UHF spectrum. The amateur radio service has frequency allocations as follows:

- 50-54 MHz (also known as the 6 metre band, but in some regions only 50-52 MHz is available due to restrictions). This band provides good ground wave propagation beyond line-of sight covering up to about 100 km. Depending on propagation conditions, this band can be subject to interferences from sky-wave signals.
- 144-148 MHz (2 metre band, restricted in some regions only to 144-146 MHz).This band is the best choice for local communication between hand-held transceivers within coverage of up to about 10 km or up to about 30 km with directional antennas. Radio amateurs are most likely to have fixed, mobile and hand-held transceivers for this band. Communication over a wider area is possible using a repeater installed in a favourable location with sufficient height over average terrain. Repeaters can furthermore be equipped with telephone interconnection devices (known as auto patch).
- 420-450 MHz (70 centimetre band, available in some regions only within 430-440 MHz). This band covers ranges shorter than those for the 2-metre band but otherwise has similar characteristics, including the possibility to use repeaters.
- Several bands in the range between 1 and 50 GHz. These bands have applications primarily for broadband, and point-to-point data links

5.2.2 Medium-range networks

Typically provide communication from the site of an event to organisational and administrative centres outside an affected area, or to headquarters of response providers in neighbouring countries. They also ensure communication with vehicles, vessels and aircraft operating outside the coverage of available VHF or UHF networks. Communication at medium distances of 100-500 km may be accomplished by near-vertical-incidence sky wave (NVIS) propagation at the lower HF frequencies of up to about 7 MHz. The band characteristics are as follows:

- 1 800-2 000 kHz (160 metre band): This band is most useful at nightime and during low solar activity. Under field conditions, the dimensions of antennas may restrict the use of this band, which is also frequently affected by atmospheric noise, particularly in the tropical zone.
- 3 500-4 000 kHz (80 metre band, only available in some regions within 3 500-3 800 kHz): This is an excellent nightime band. Like all frequency ranges below about 5 MHz it can be subject to high atmospheric noise.
- 7 000-7 300 kHz (40 metre band, in some regions available within 7 000-7 100 kHz): This is an excellent daytime band for near-vertical-incidence sky wave paths. At the higher latitudes, especially during periods of low sunspot activity, lower frequencies may be preferable. In view of this band’s importance for amateur radio emergency communications, the World Radio-communication Conference WRC-03 (Geneva, 2003) has initiated the process to increase the allocations in regions so far limiting the band to less than 300 kHz, and some national administrations have already implemented an increase from 100 to 200 kHz).
- In the 5 MHz range, several national administrations have allocated fixed frequencies (channels) for amateur radio emergency traffic and related training. The 5 MHz range allows the most reliable links in the medium range during 24 hours per day and under most propagation conditions.

5.2.3 Long-range networks

Ensure the links with headquarters of international emergency and disaster response providers. They also serve as backup connections between offices of such institutions in different countries or on different continents. Amateur stations routinely communicate over long distances, typically beyond 500 km, using oblique-incidence sky wave propagation in HF. The characteristics of the respective bands are as follows:

- 3 500-4 000 kHz (80 metre band, available in some regions within 3 500-3 800 kHz): This is an excellent nightime band, particularly during low sunspot activity. However, communications may be affected by high atmospheric noise, particularly at low latitudes.
- 7 000-7 300 kHz (40 metre band, which is available in some regions within 7 000-7 100 kHz): This band is a good choice for up to around 500 km during daytime and for long distances, including intercontinental paths, at nightime.
- 10 100-10 150 kHz (30 metre band): The 30-m band has good day and night propagation and can be used for data communication. It is not currently used for voice because of its limited width.
- 14 000-14 350 kHz (20 metre band): The 20-m band is the common choice for the daytime communication over long distances.
- Propagation on the following bands is suitable for longer distances during daytime and high sunspot activity:
  - 18 068-18 168 kHz (17 metre band)
  - 21 000-21 450 kHz (15 metre band)
  - 24 890-24 990 kHz (12 metre band)
  - 28 000-29 700 kHz (10 metre band)

5.2.4 Amateur radio satellites

Can serve as an alternative to HF sky wave links for medium and long-range communication. The amateur radio service does not at this stage operate geostationary satellites or interlinked satellite constellations. Its satellites not therefore provide continuous global coverage, but in some cases the storage-and-forward capability allows the forwarding of messages between stations without simultaneous access. Further developments in the amateur radio satellite service is be expected to increase its applications in emergency telecommunications. The amateur radio satellite service uses specific frequencies within the allocated bands, mostly in the VHF range and above. Communication over some satellites is possible with low power equipment and with low gain antennas.

5.3 Operating frequencies

Different from most other services, the amateur radio service enjoys the privilege of band allocations, the use of which is left to the self regulation of the amateur radio associations. Flexible use of the rare commodity of frequency spectrum thus allows particular flexibility in operations.

The allocated frequency bands are described and their characteristics given in 5.2. above. The choice of the most suitable frequency band and of the most convenient channel within the selected band is, given in the band plans prepared by the IARU, and choice is prerogative of each individual operator. In emergency situations, any radio station can establish contact on any frequency that it can technically operate on. In such a situation, stations of the amateur radio service can be contacted, or can initiate contacts with, stations of other services such as the maritime or the land fixed or mobile service.

In some countries, specific frequencies (channels) have been defined as emergency frequencies. Due to the dynamic use of frequencies within the allocated amateur radio bands, a permanent reservation of such channels outside times of acute emergencies is however problematic and a restrictive policy in respect to the use of the available spectrum might prove counter-productive. In some cases, national administrations have assigned frequencies adjacent to the allocated amateur radio bands to disaster response organizations, thus facilitating communications with stations of this service and allowing the use of amateur radio equipment and antennas with ease.

5.4 Communication modes

Stations of the amateur radio service are authorized to use a wide variety of transmission modes, provided the allocated frequency bands, IARU and national band plans, and national regulations provide the bandwidth needed for the particular mode chosen. The selection of the appropriate mode in any specific case depends on numerous factors, including volume and nature of the information to be transmitted, technical specifications of the equipment available and the quality of the communications link. The following communication modes are most commonly used in the amateur radio service as well as in other services such as the maritime and the fixed and land mobile services:

- ***Radio telegraphy:*** Use of the international *Morse code* is still widespread throughout the amateur services and can play an important role in disaster communications, particularly when only elementary equipment or low transmitter power are available. The use of Morse code also helps to overcome language barriers in international telecommunications. Its effective use requires operators with skills greater than the minimum licensing requirements.

- ***Data communications:*** These have the advantage of accuracy and of creating records for later reference. Messages can be stored in computer memory or on paper. Digital data communication requires additional equipment such as a desktop or laptop computer communication interface, processor or modem. The communication processor performs encoding and decoding, breaks the data into transmission blocks for transmission and restores incoming data into a stream. It also compensates for transmission impairments, compresses and decompresses data, and handles analogue-to-digital and digital-to-analogue conversions.
- ***HF (shortwave) links:*** The Amateur Radio Service uses a variety of data communications *protocols*. PACTOR II and III is one of the common modes available for amateur disaster communications and is also used on emergency networks of the United Nations and other organizations. Depending on the specific requirements of a network, other data modes are available, among them PSK-31, a real-time data communications mode, replacing the radio teletype (RTTY) links used in the past.
- ***Packet radio:*** This is a powerful tool for traffic handling. Text messages can be prepared and edited off-line then transmitted in shortest time, thus reducing congestion on busy traffic channels. Packet radio can be used by fixed as well as mobile or portable stations. This is an error-correcting mode and uses the radio spectrum efficiently. It allows multiple communications on the same frequency at the same time by using time-shifting communication. By storing messages on packet bulletin boards (PBBS) or mailboxes, stations can communicate with other stations not on the air at the time. Packet radio operates over permanently established or temporary networks. The AX.25 packet radio protocol is a reliable and efficient method of data communications at rates of 1 200-9 600 bit/s, depending on the equipment used.
- ***Suppressed-Carrier Single-Sideband (SSB) radiotelephony:*** This is the most commonly used mode for HF (shortwave) voice radio links. Due to its high efficiency and narrow bandwidth, SSB has replaced the previously used amplitude modulation (AM) in all services using HF except the broadcast service. It can however only be received by equipment designed for this mode and not by ordinary broadcast receivers. Due to the narrow bandwidth, the voice signal might be somewhat difficult to understand for untrained ears. On frequency ranges, where more bandwidth is available, another voice mode is more common.
- ***Frequency modulation:*** This is used in local and regional fixed and mobile networks. It has the advantages of high audio quality and resistance against interference such as caused by vehicle engines and is therefore the communication mode of choice on local VHF and UHF networks.
- ***Image communications:*** The Amateur Radio Service supports two more modes that make the transmission of facsimile and television possible. In emergency situations, television images can provide valuable information from the site of an event. Analogue image communication modes are now generally replaced by the transmission of images as digital files using data modes.

5.5 Repeater stations

Repeater stations or relays are used to extend the communication range of VHF and UHF stations. Positioned in elevated locations they allow communication between fixed or mobile stations separated by obstructions such as mountains or tall buildings when operating in an urban environment. A repeater station receives on one channel and transmits on a different frequency, usually within the same band. Filters, so called duplexers, prevent interference between its simultaneously operating transmitter and the receiver. Important considerations for the location of a repeater station are not only its geographical coverage, but also its power requirements. Rechargeable batteries, supplied from solar cells or wind generators are the most common solutions.

Special forms of repeaters are the analogue or digital transponders used in the amateur radio satellite service. Like terrestrial relays, they re-transmit a received signal on a different frequency; their geographical coverage or "footprint" is however much larger. Transponders on board of balloons or aircraft have successfully been used by radio amateurs and might in the future become available as an additional tool for emergency telecommunications. Digital transponders have the capability to store received messages, and to re-transmit them on demand, at the time when the receiving station is within their range.

5.6 The organization of the amateur radio emergency service

The amateur radio service is a continuous activity. At any given time, at least some networks and operators of this service are available and can assume a role in emergency telecommunications without delay. Additional resources can be mobilized on very short notice. For an efficient application of the service to emergency and disaster response, a higher degree of preparedness, including training, exercises and mobilization procedures, is desirable. Cooperation with the International Telecommunication Union has facilitated the training of some radio amateurs on the African continent in the past.

The structures of cooperation between the amateur radio service and the national authorities, emergency services and disaster response providers, depend on the situation in each country. The outline presented in the following sections is mostly based on the concepts used in the USA. The general principles should however be applicable in most parts of the world. In all cases, decisive factors include the number of amateur radio stations involved and the number of certified operators, as well as the structures of national response mechanisms.

5.6.1 The Amateur Radio Emergency Service (ARES) groups

Amateur Radio Emergency Service groups, in several countries known as ARES, consist of licensed amateurs who have voluntarily registered their qualifications and equipment for communications duty in the public interest. All licensed amateurs are eligible for membership in the ARES. Members of ARES groups either use their own personal emergency-powered equipment, or operate equipment that the group has acquired and maintains specifically for emergency telecommunications. The outline of standard ARES procedures given in the following section may also serve as a guideline for emergency telecommunications support teams in general. The following important points must be noted:

- *Preparedness* requires, that team members are familiar with the functions they are expected to assume and prepared to do on shortest notice. Credentials should be provided for recognition by local authorities. If possible, an ARES activation should start with an operational and a technical briefing, based on information received from the requesting authority and supplemented by reports from amateur radio, media, and other sources. The briefing must include an overview of identified equipment and manpower requirements, hierarchical structures, ARES contacts, and conditions to be expected in the affected area.

- *Travel time* spent on the way to a disaster-affected location should be used for review of the situation with the team. The review should include task assignments, checklists, affected area profile, mission disaster relief plan, strengths and weaknesses of previous and current responses, maps, technical documents, contact lists, tactical operation procedures, and response team requirements.

- *Upon arrival*, team leaders should check with local ARES officials and obtain information on frequencies in use, current actions, available personnel, communication and computer equipment, and support facilities. The ARES plan in effect for the specific disaster should be obtained. Priority should be given to the establishment of an initial intra-team communication network and HF or VHF links to the home location. Team leaders should meet with served agencies, amateur radio clubs' communications staff, local communications authorities and others as needed to obtain information and coordinate the use of frequencies. Communication site selections should take into account team requirements and local constraints.

- *During operations* team leaders should continuously assess the operational status of regular communication facilities and of the networks of other response teams, to coordinate operations and avoid duplications. Proper safety and security procedures must be followed. Periodic reviews of communication effectiveness should be conducted with served units and communication personnel.

- *An exit strategy* for amateur communicators needs to be in place from the beginning of an operation. It needs to be negotiated with served agencies and host officials in time. To obtain volunteers' commitment to travel and participate, they must be assured that there will be an end to their commitment. Leaders must coordinate with served agencies in determining when equipment and personnel are no longer needed. A demobilization plan needs to contain clear definitions on the handover of responsibilities. A debriefing should be conducted at the earliest possible time and might include individual performance evaluations. Problems stemming from personality conflicts should however preferably be addressed and resolved outside of formal reports, as they provide distractions to the reports. Equipment should be accounted for. Lessons learned need to be documented and be made available for broader review, comments and use in future training and preparedness activities.

- *Standard Operational Procedures (SOP)* are a key element in all emergency operations. In emergency telecommunications such SPO need to be in place in particular on message format and handling, the use of simplex channels, repeater operations, and on station identification. Following such standard principles of operations is preferable to the introduction of new and possibly not previously exercised ad hoc procedures.

- *Amateur radio operators do not need training on basic communication skills* or general technical matters. They do however need to become familiar with the operational environment and with the partners they serve with. Proper disaster training needs to prepare the participants for systematic and accurate work in even the most chaotic environment. The moto should be, "It's people who communicate, not radios".

- *Training* should focus on the following subjects: emergency telecommunications, traffic handling, net or repeater operation, and technical knowledge. Practical on-the-air activities, such as a Field Day or a Simulated Emergency Test (SET) offer training opportunities on a nationwide basis for individuals and groups and reveal weak areas in which more training or improvements to equipment are needed. In addition, drills and tests can be designed specifically to check the readiness and the reliability of emergency equipment that is not permanently in use. A drill or test that includes interest and practical value makes a group motivated to participate because it is purpose or goal oriented. In order to present a realistic scenario, training should be centred on a simulated disaster situation and, if possible, in combination with training exercises of other partners in emergency assistance.

- *Exercises* should include the activation of emergency networks; including the assignment of mobile stations to served agencies, the originating and processing of messages and the use of emergency-powered equipment. As warranted by traffic loads, liaison stations may need to be assigned to receiving traffic on a local network and relay it to outside destinations. To a large degree, the value of any exercise depends on its careful evaluation and on the application of lessons learned.

- *Field Day (FD) events* are a traditional form of exercise with a competitive character. During a field day, radio amateurs operate under simulated emergency conditions. A premium is placed on operating skills and adapting equipment to meet the challenges of emergency conditions and related logistics. Amateurs are used to operate stations capable of short, medium and long-range communications at almost any place and under difficult conditions. Essential is the use of other sources of energy other than commercial power. Use of generators, batteries, wind, and solar power is an important element in this whole exercise.

- *Simulated Emergency Test (SET)* builds emergency-communications skills. SET help operators in gaining communication experience in using standard procedures under simulated emergency conditions, and to experiment with some new concepts. Issues to remember about SET are that it:

  – determines strong points, capabilities and limitations in providing emergency communications to improve the response to a real emergency,

  – provides a demonstration, to served agencies and the public through the news media, of the value of amateur radio, particularly in time of need,

  – exercises VHF-to-HF interfaces at the local level,

  – encourages an increased use of digital modes for handling high-volume traffic and point-to-point welfare messages,

  – strengthens the cooperation between amateur radio operators, users and disaster response organizations, and

  – focuses energies on ARES communications at the local level, on the use and recognition of tactical communications, and on the procedures for formal message traffic.

- *Traffic handling* includes the forwarding of messages from and to others outside the circle of amateur radio operators. Where national regulations allow, amateurs radio stations can handle such third party traffic both in routine situations and in times of disaster. Such public-service communications make amateur radio a valuable public resource and provide the best training for emergency telecommunications. The traffic network structures differ in the various countries, but the outline given in the following section may serve as an example:

  – *The Tactical Net*work is the frontline net activated during an incident. Such a net is often used by a single government agency to coordinate with amateur radio operations within their jurisdiction. There may be several tactical nets in operation for a single incident depending on the volume of traffic and number of agencies involved. Communications typically include both traffic handling and resource mobilization.

  – A *Resource Network* may be needed to recruit operators and equipment in support of operations on the Tactical Networks in large scale operations. As an incident requires more operators or equipment, the Resource Network evolves as a check-in place for volunteers to register and to receive their assignments.

- A *Command Network* may become necessary if the dimension of a disaster response operation increases and more partners become involved in the incident. This network allows incident managers to communicate with each other to resolve inter- or intra-agency problems, particularly between cities, or within larger operational areas. It is conceivable, that such a network becomes overloaded over passage of time due to high traffic volume. It may consequently be necessary to create multiple command nets to cover all requirements.

- *Closed networks* operate with a network control station responsible for overseeing the flow of communications. When the amount of traffic is low or sporadic, such a network control function may not be required. In an open network, participating stations simply announce their presence and remain on standby. If they have traffic, they directly call another station after checking that the channel is not presently occupied. In a closed network, any station wishing to establish a contact, calls the network control station for authorization. The network control station might either authorize direct communication on the calling channel or assign a working channel to the respective stations. Upon completion of their communication, the participating stations report to the network control station on the main frequency. For this type of operation, it is essential that the network control station keeps a record of the activities of all stations and of working channels assigned. This will ensure that all stations remain continuously available for urgent messages.

- *Network discipline* and message-handling procedures are fundamental concepts of amateur radio network operation. Training should involve as many different operators as possible in network control station and other functions. The basically informal character of amateur radio operations makes it necessary to pay particular attention to the procedures for handling messages within and among the different networks and between the amateur radio service and other networks. Permanently established traffic networks are ideal means to ensure efficient message handling during an emergency.

- *An Emergency Operations Centre (EOC) or Command Post (CP)* is usually established by the authorities in charge of a disaster response operation. The CP primarily controls the initial activities in emergency and disaster situations, and is typically a self-starting, spontaneously established entity. The initial functions of the CP are to assess the situation, to report to a dispatcher and to identify and request appropriate resources. The Emergency Operations Centre (EOC) responds to requests from a CP by dispatching equipment and personnel, anticipating needs to provide further support and assistance and pre-positioning additional resources in a staging area. If the situation at the site of the event changes, the CP provides the EOC with an update and maintains control until the arrival of additional or specialized resources. By being located outside the perimeter of potential danger, the EOC can use any appropriate type of communications, concentrate on gathering data from all partners involved, and mobilize and dispatch the requested means of response.

- *The format* chosen to handle traffic on a network depends on operational conditions and its selection requires knowledge of the possibilities and limitations of the telecommunications resources available. Tactical traffic supports the initial response operations in an emergency situation, typically involving few operators within a limited area. Tactical traffic, even though unformatted and seldom written, is particularly important when different organizational entities are getting involved in the operations. The use of one VHF or UHF calling frequency, including possibly the use of repeaters and network frequencies, characterize most typical tactical communications. One way to make tactical network operation transparent is to use tactical call-signs, i.e. words that describe a function, location or agency, rather than call-signs of the Amateur Radio Service. When operators change shifts or locations, the set of tactical calls remains the same. Call-signs like “Event Headquarters”, “Network Control” or “Weather Centre” promote efficiency and coordination in public-service communication activities. Amateur radio stations must however identify their stations at regular intervals with the assigned call signs.

– *Formal message traffic* is handled in a standard message format and primarily on permanently or temporarily established HF and VHF networks. There may be links between local, regional and international networks. When accuracy is more important than speed, formatting a message before it is transmitted increases the accuracy of the information transmitted. Packet radio is a preferred mode for the handling of formal messages. It also allows the forwarding of traffic between various networks with a minimum of re-formatting, thus ensuring accuracy.

Health and welfare traffic is, for those affected by a disaster, of highest importance. The need to communicate may be less dramatic than the loss of one’s home, but just in extreme situations a loss of such basic commodities as access to a telephone is felt very much. Secondary to the priority traffic of emergency response services, the handling of welfare traffic as a service to the public and often originating from places evacuees at shelters or at hospitals is a task of the amateur radio service. Incoming health-and-welfare traffic should always only be handled after all emergency and priority traffic is cleared. Answering welfare inquiries can take time and questions might have already been answered through restored circuits. Stations at shelters, acting as network control stations, may exchange information on the HF bands directly with destination areas as propagation permits. They may also handle formal traffic through outside operators.

5.6.2 Typical situations for amateur radio emergency communications

Despite the wide spectrum of requirements in a disaster situation, amateur radio operators should neither seek nor accept any duties other than those foreseen in the agreements on their status in an emergency operation. Volunteer communicators are not the decision makers in relief operations, and they are not normally qualified or authorized to take on responsibilities beyond those of communicators. The amateur radio service provides communications in support of those who provide the actual emergency response. Operators with skills in other fields such as search and rescue or first aid and affiliation to respective organizations need to decide in advance, which role they wish to accept within an operation.

- *Initial Emergency Alerts* may originate from individual amateur radio operators using their equipment and networks to bring an incident to the attention of the competent institutional emergency services. Using their VHF hand-held and mobile radios, radio amateurs might activate a repeater autopatch code, connecting a repeater to a telephone line. By dialling an emergency number, the operator has direct access to the respective services.
- In *Search and Rescue* operations, operators of the amateur radio service can reinforce the professional teams by increasing their communication capabilities but also by making and reporting own observations.
- *Hospitals* and similar establishments might in the aftermath of a disaster be without communications. This affects in particular the coordination among various providers of health services. Inside a hospital, ARES operators might temporarily serve as replacement to a paging system and maintain critical interdepartmental communications. Local amateur radio emergency groups should prepare in advance for such hospital communications and ARES groups should be familiar with the communication structures they might be asked to replace.

- *Chemical Spills* and other incidents involving hazardous materials may require the evacuation of residents and the coordination between the disaster site and the evacuation sites or shelters. The term “hazardous materials” (HAZMAT) refers to substances or materials which, if released in an uncontrolled manner, are harmful to people, animals, crops, water systems, or other elements of the environment. The list includes explosives, flammable and combustible gases, liquids and solid material, oxidizing, poisonous and infectious substances, radioactive materials, and corrosives. The initial problem in an incident with such materials is the determination of the nature and quantity of the chemicals involved. Various institutions maintain registers of hazardous materials in order to provide rapid indications of the hazards associated with potentially dangerous substances, but this most essential information will not be available unless communications can be established immediately. ARES operators may be asked to establish communications with such institutions. Information on potential and real information sources, as well as the standard markings of hazardous goods and basic safety procedures should therefore be included in the briefing material of ARES groups.

5.7 Third-party communications in the Amateur Radio Service

Under normal circumstances an, amateur radio communication connects two parties communicating with each other. In emergency situations, operators will be requested to pass a message on behalf of a third party, a person or organization that is not necessarily present at the radio station.

From the regulatory point of view, two cases need to be distinguished: If both sides of the radio link are within a single country, third party traffic is subject to national regulations. If the message originates from an amateur radio in one country but is destined for a third party in another country, the Radio Regulations (RR) of the ITU concerning international third party traffic need to be respected. They provide that, in the Amateur Radio Service such traffic is allowed only if a bilateral agreement exists between the national Administrations concerned, or in case of emergency operations and training for such. Some administrations may tolerate third party traffic or enter into temporary agreements if this type of traffic is in public interest, such as when other communication channels have been disrupted.

Operators should be aware that it is a general rule for all radio communications that when safety of life and property is at stake, administrative regulations can be temporarily waived. Article 25 of the Radio Regulations, governing the amateur radio service, has been revised by the World Radiocommunication Conference (WRC-03, Geneva, 2003) to the effect, that third party traffic is authorized for emergency operations and related training.

5.8 Optimizing the use of the Amateur Radio Service as a public service

The amateur radio service is occasionally considered as a thing of the past. This mistaken impression may stem from its name, which distinguishes it from all other radio services. It is however just this distinction that expresses the value of this service in times when other communication capabilities are lost. The amateur radio operator is able to communicate using the widest variety of tools, and the amateur radio service often makes the difference between “no communication” and a maybe less user-friendly, but functioning communication service. The fact that personal mobile communications are becoming readily available to the majority of the people worldwide does not make their users skilled communicators; they are consumers, and not active participants. In an emergency situation, communication such as that provided by radio amateurs continues to play a critical role. It is up to the national administrations and to the providers of emergency response, to keep making best use of this time proven, invaluable resource.

CHAPTER 6

Broadcasting

6.1 Broadcasting

Broadcast (Radio and TV) is a very powerful means to reach large sections of the public with information and advice. National regulations and customs differ from place to place as to how information is given to the public.

In some cases, the broadcaster allows only content created by their own staff, to be transmitted. Own presenters, principally news anchors, will make the announcements over the air. They will initiate a “News Flash” for this purpose, and interrupt normal programming. Journalists like to establish links with “Reliable Sources” in advance, so that they know who is the spokesperson for the government.

Governments need to understand that journalists are trained to gather and then spread information, so if government spokesmen are giving out old and inaccurate information, journalists tend to dig and search information by themselves. To the citizens, the government will look slow and incompetent if all the details only come from the independent journalist. Since this may backfire after the event, it is important to engage with the media very early providing as accurate and timely information as possible.

Today, there is also a tendency for news journalist to want to appear to be “on the spot”. They often quote commentators close to the scene of the event rather than those in the studio located in the capital. For this reason, there is need for government to move with this trend by setting up “media cities” close to the incident, but out of the “Hot Zone”. The media need locations for their cameras (preferably one where they can see the Hot Zone) and where their communications trucks can be safety sited. Creating a place where well informed spokespersons are located, and there is food, drink, power and broadband telecoms encourages the media to get its information from the right sources rather that from some uniformed and unreliable sources.

The Emergency Alert System (EAS), as is used in the USA is an example of another approach. By government mandate or voluntary participation, broadcasting stations are connected to an EAS data communications system. If there is an alert, a data burst is sent to the TV or radio stations in the countries concerned. In most cases, the running programme is interrupted by a data burst transmitted over the air. People can buy a decoder to read what the message says. Even radios playing pre-recorded music are interrupted with a special alert message. Today, most countries use this facility to warn drivers on road and traffic conditions. In the case of TV stations, a scrolling text bar can appear across the screen making clear text announcements.

Remote “opt out” is a system whereby a local radio station, (this may be automatic at night), can be controlled by another studio, say in the capital city. Local radio stations are often controlled by a clock, which switches to the big studio at news time, then back to local content at other times. By means of an opt out system, the main studio can cause the local station to stay connected to the news studio until the emergency announcements have been completed. The problem is that the local radio station may as a result fail to fulfil its obligation to transmit scheduled advertisements thus losing revenue. Some sort of agreement about this before it is done is required.

To ensure that this service is active all the time, planners should arrange for back up power and secure communications for broadcasting transmitters and their studios.

6.2 Mobile emergency broadcasting

Mobile radio stations can be quickly and cheaply moved into the affected area. However, locals should have powered radios or even wind up radios for them to be able to turn in. This is an efficient way of reaching out many people in the shortest time. However, there are a lot of political considerations to take into account.

Full consultation with relevant government authorities is imperative. Some governments are concerned about a free flow of information in times of national crisis. The concern is that certain broadcasts can cause panics if not well crafted.

CHAPTER 7

New technologies and new practices

7 Recent developments

This segment summarizes what have emerged as new ways of managing information in times disasters or impending disasters.

a) Cell broadcasting was discussed in previous chapters on mobile networks. Increasingly, there is use of SMS-CB to broadcast information. SMS-CB causes short text messages in selectable languages to appear on the screen of the mobile phone, and then set off the alert tone. Advantages of SMS-CB vs. normal SMS.

   – It transmits to everyone at the same time, taking about 20 seconds to deliver.

   – It does so over dedicated broadcast channels, and thus neither causes, nor is affected by overload of the network.

   – The sender of the message can select a single cell, or any number of cells to make the area of warning as big or as small as is required.

b) Cellular Emergency Alert Systems Association (CEASA) is one international organisation that is seeking to develop and deploy a network of government-to-citizen warning systems, which deliver messages to users via cell broadcast.

c) IP telephony is growing in popularity. It should be noted that a normal Internet application such as email or the web browser is not very sensitive to delays. Voice on the other hand is very sensitive to delay and will cause unintelligible words breaking if there are delays on the route. Unlike conventional networks, IP packets can be stored in routers being queued for outgoing transmission. During an emergency, loading may make the output queues quite long and some packets may be discarded. IP telephony does not use TCP to request for a new packet resulting in the chopping of voices. The only way to avoid this is to use a well managed IP network to keep the loading and delays down to the barest minimum.

d) DVB

   Digital video broadcast uses TV satellites to provide Internet access. It has the advantage of being significantly cheaper than conventional systems, but like any IP based system, suffers from contention at busy times. In other words it may be used with difficulty in times of emergencies.

e) ISTOS

   ESA’s concept for an Integrated Space Technologies Operational System (ISTOS) Wide Area Network. It is designed to improve the utilisation of space technologies by end users working in the field of emergency management, by allowing the efficient interconnection of emergency application users to data and service providers, using integrated space technologies in telecommunications, earth observation and navigation.

f) STANAG is an emerging standard for HF data radio. This is a NATO standard for 9.6 kbit/s data over HF. Its deployment in emergency situations is yet to be tested.

g) Digital trunked radio systems

We are witnessing the deployment on a wide-scale of digital trunked radio systems such TETRA (system offering advantages in terms of clarity, wide-area coverage, rich terminals and high security). In general the following are key elements associated with these systems:

– The old analogue systems were notoriously insecure and easy to listen into unless a secure encryption system was used. Digital systems normally feature very robust security such that even if a casual listener were to tune-in, data would appear as garbage.

– All terminals are uniquely identifiable. These will not be granted access to the system unless they are valid on that particular system and on the requested talk groups. In addition, each terminal can be remotely stunned or killed in case of it being lost. There is therefore no risk of an unauthorized person using a lost and found terminal.

– Digital systems are capable of transmitting both voice and data. They are also capable of point-to-point connection as well as mobile phone like through connection.

– Thanks to voice coding and compression, modern systems have up to 4 times more capacity than analogue services. As a result, there are more talk groups available thus remarkably reducing congestion.

– Whereas the traditional systems arranged talk groups on geographical basis, due to the need to use repeaters, trunked systems eliminates this problem making it possible to deploy talk groups on tactical basis which is much more convenient.

– Signals are cleaner and clearer thanks to speech coding and noise including squelch noise are eliminated thanks to speech coding.

– Many systems such as TETRA have a "simplex" mode otherwise known as "direct mode".

– Trunked networks can take the form of simple stand-alone repeaters or form more complex national networks. In disaster operation, it is advisable for several agencies to club together to build a single wide-area-network. There remains an option for the agencies to maintain separate talk groups or to have inter-agencies common talk groups that make and facilitate coordination. This however, requires that terminals are available to all agencies. Interworking could be a solution as terminals could be made available at least in the control room of other agencies. This is however, a subject yet to be dealt with by senior management at agency level as it posses a lot of challenges.

PART III

Technical Annex

Some technical aspects of
disaster communications

1 Introduction

In Part 1 of this Handbook, the reader was presented with definitions and overall policy considerations regarding disaster communications. Following this general discussion, the reader was invited to consider the more specific guidance required to operate an emergency telecommunications network as presented in Part 2 designed for operational personnel.

In order to improve the flow of thought in Parts 1 and 2, technical details and formulas are consolidated in Part 3. This permitted the previous two parts to be written in a narrative style. Further, it made the text more readable for planners and policy-makers who require an overview of the problems, solutions and techniques related to emergency telecommunications.

Part 3 is organised into the following sections:

- The selection of the appropriate technology for emergency telecommunications
- Methods of radiocommunication
- Antennas as an essential part of any radio station
- Use of relay stations (repeaters) and trunking systems
- Power sources (including batteries)

In addition, there is a bibliography listing a number of references that will guide the reader to an extensive historical source listing. Also, it will provide information about useful sources of additional information from which it is possible to expand on the subjects raised in briefer form in this Handbook.

At the conclusion, there is an Appendix of a number of useful documents from a number of diverse original sources.

2 The selection of appropriate technologies for emergency telecommunications

2.1 Simplicity vs. new technologies

Generally, the simpler time-tested forms of radiocommunication work best in disaster situations. These include single-sideband (SSB) voice and Morse code (CW) telegraphy at HF and FM voice at VHF/UHF.

The equipment has been perfected over time, and its installation, maintenance and operation are widely understood. There are robust versions of equipment designed to meet the rigours of transportation and operation in the field.

Nevertheless, some newer technologies offer features that may facilitate emergency telecommunications. Those include cellular telephones, digital dispatch radios, facsimile, data communications, television and satellites. Each has their advantages and disadvantages, which should be weighed carefully in the planning process.

Emerging technologies such as 3rd generation cellular (IMT-2000), software-defined radio (SDR), broadband and multimedia systems should be evaluated in terms of their ability to function during emergency conditions.

Training of radiocommunication personnel is an important aspect of the selection of appropriate technologies. It is fruitless to plan on an HF Morse telegraphy capability without trained and experienced operators. Use of SSB voice to avoid training Morse operators is not necessarily a solution unless the operators are trained in installation, maintenance and operation of an SSB radio station. It is also inappropriate to introduce new technologies without a continuing supply of personnel adequately trained in system planning, installation, maintenance and operation.

The ideal emergency telecommunications system is one in routine daily use that has the capability of functioning in disaster and other emergency conditions. Second best is a capability exercised periodically, such as weekly or monthly, under simulated emergency conditions.

2.2 Reliability of the infrastructure

HF communications, whether by SSB voice or Morse telegraphy, normally do not require any infrastructure for relaying or processing. Communication is usually a direct link between the originating station and the addressee. When long distances are involved, such as beyond 2 000 km, or when propagation conditions are poor, base stations or relay stations can be used to facilitate communication but may not necessary be required.

2.3 Transportation and mobility considerations

New technology includes such telecommunication systems as portable satellite earth stations, mobile and portable cellular telephone base stations, and telemedicine video base and remote stations. There are circumstances where it would be desirable to use these new technologies at a disaster area. However, transportation and mobility should be taken into account before using such systems. For example, a satellite earth station that is mounted on pallets requiring special handling equipment for loading and unloading because an aircraft may be available at the point of origin, but not at the point of debarkation.

Further, once the communications system is unloaded at the nearest available airport, ground transportation will be needed to transport it to the disaster area. Trucks and loading equipment are generally in full use at the disaster site and may not be available at an airport.

A third consideration is the condition of roads leading to the disaster area. In many cases, it may not be possible to move the communications equipment to a location where it is most desired because of obstructions.

2.4 Interoperability

The capability to communicate with the local public protection organisations such as police, fire and medical, the local military, international disaster relief organisations and neighbouring countries is an important consideration.

There may be circumstances where it should be possible for any station to be able to communicate with any other station in the disaster area. Such a feature can cut across the formal structure and get communications directly to the intended party without experiencing delays and possible misinterpretation by intermediaries. Unfortunately, there are other circumstances where separate channels are needed for different groups of stations and it would be difficult if not impractical for everyone to be on one channel.

2.5 Comparison of satellite systems for emergency telecommunications

2.5.1 Low Earth orbit satellites

Low Earth orbit (LEO) satellites may be used to relay radio signals far beyond line-of-sight. Depending on altitude, a single LEO satellite could be used to relay signals over paths up to about 5 000 km when the two earth stations are both visible to the satellite. Such visibility lasts only for a few minutes at such extreme distances. Stations closer together can have mutual visibility to the satellite for longer periods, perhaps up to 20 minutes on a favourable pass. Owing to their orbits, single LEO satellite have the disadvantage that they can provide real time communication only for a few times a day.

LEO constellations can be used for continuous real time relay. This requires a sufficient number of satellites to assure that at least one is visible to a point on Earth at all times. Also, there must be a means of networking the satellites, either through inter-satellite (satellite-to-satellite) links or via earth stations located throughout the world.

2.5.2.1 Inmarsat vs. VSAT and USAT

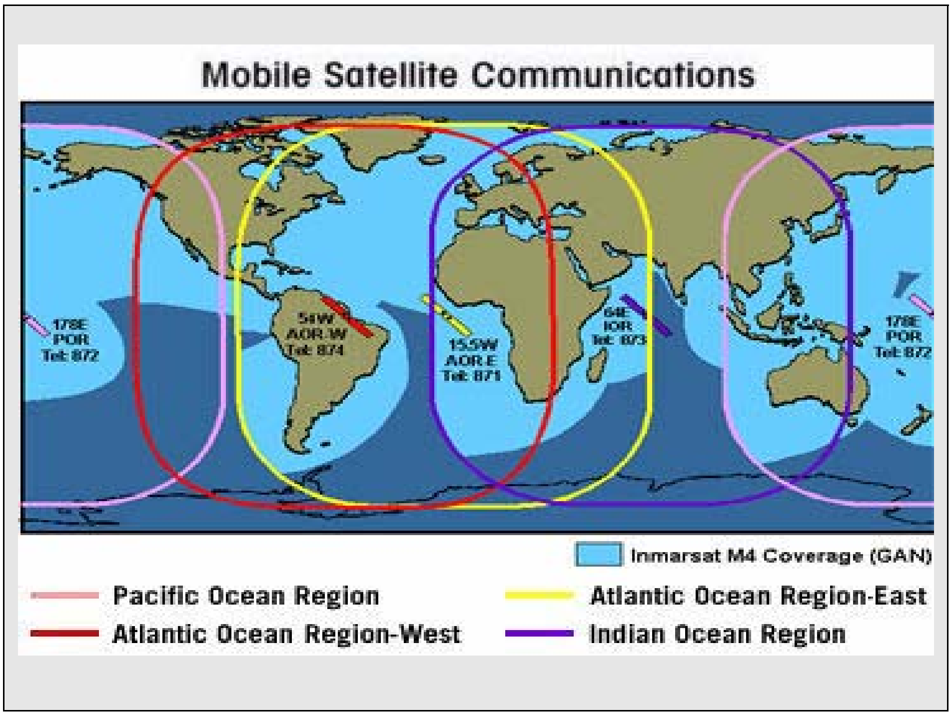
Common telephone and data services are available from land-based satellite terminal systems using the portable International Maritime Satellite (Inmarsat) or the semi-fixed Very Small Aperture Terminal (VSAT) satellite network. These services include voice, facsimile and electronic mail communications. Any device that works with a common telephone device may be used with these satellite systems. In addition to the above-mentioned services, some satellite terminals offer transfer of digital photographs or live video conferencing.

The choice of whether to use Inmarsat or VSAT is dependent upon the particular telecommunications requirements for the system. Many variable factors will influence the choice of one over the other: cost, mobility, and the need for high volume use. Also, the ability of the system to support various modes of communication, such as: standard voice, computer data (networked or stand-alone e-mail connections), facsimile, text-only messages and videoconferencing.

Inmarsat provides a global mobile satellite communications capability with several advantages to support disaster preparedness and relief operations. Inmarsat terminals are self-sufficient and can be operational within 5-10 minutes of arriving at the disaster scene. They are independent from local telecommunications infrastructures, and can be operated with batteries or generator power suppliers. Inmarsat systems can be configured to provide communications between two independent relief teams working in the same locality or to provide direct links to relief agencies and material suppliers worldwide. One important detail is that Inmarsat equipment is simple to operate, and can be set up and operated by untrained personnel using instructions provided with the units. The equipment is compact and lightweight. Some models can be hand carried.

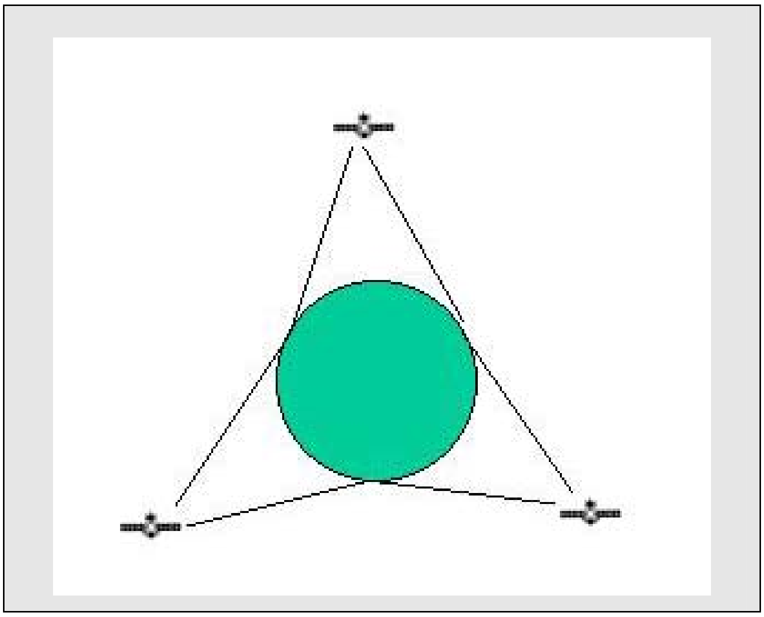
Inmarsat's primary satellite constellation consists of four Inmarsat I-3 satellites in geostationary orbit. A fifth spacecraft that can be brought in to provide additional capacity currently backs these up. Between them, the main "global" beams of the satellites provide overlapping coverage of the whole surface of the Earth apart from the poles. So, with Inmarsat coverage, it has become possible to extend the reach of terrestrial wired and cellular networks to almost anywhere on Earth.

Figure 2 – Mobile satellite communications



A geostationary satellite follows a circular orbit in the plane of the Equator at a height of 35 600 km, so that it appears to hover over a chosen point on the Earth's surface. Three such satellites are enough to cover most of the globe, and mobile users rarely have to switch from one satellite to another. Other mobile satellite systems use larger numbers of satellites in lower, non-geostationary orbits. From the user's point of view, they move across the sky at a comparatively high speed, often requiring a switch from one satellite to another in mid-communication and risking the possibility of an interrupted call.

Figure 3 – Three satellites in geostationary orbit can cover the entire Earth



The satellites are controlled from the Satellite Control Centre (SCC) at Inmarsat HQ in London. The control teams there are responsible for keeping the satellites in position above the Equator, and for ensuring that the onboard systems are fully functional at all times.

Data on the status of the nine Inmarsat satellites is supplied to the SCC by four tracking, telemetry and control (TT&C) stations located at Fucino, Italy; Beijing in China; Lake Cowichan, western Canada; and Pennant Point, eastern Canada. There is also a back-up station at Eik in Norway.

A call from an Inmarsat mobile terminal goes directly to the satellite overhead, which routes it back down to a gateway on the ground called a land earth station (LES). From there the call is passed into the public phone network.

The Inmarsat I-3 satellites are supported by four previous-generation Inmarsat-2s, also in geostationary orbit.

A key advantage of the Inmarsat I-3s over their predecessors is their ability to generate a number of spotbeams as well as single large global beams. Spotbeams concentrate extra power in areas of high demand, as well as making it possible to supply standard services to smaller, simpler terminals.

Inmarsat I-2 – Purpose-built quartet

Launched in the early 1990s, the four second-generation satellites were built to Inmarsat specification by an international group headed by British Aerospace (now BAE Systems).

The three-axis-stabilized Inmarsat I-2s were designed for a 10-year life. Inmarsat-2 F1 was launched in 1990 and is now located over the Pacific, providing lease capacity. F2, launched in 1991, is over the western Atlantic, providing leased capacity and backing up Inmarsat I-3 F4. Also orbited in 1991, F3 is stationed over the Pacific Ocean, providing lease capacity and backing up Inmarsat I-3 F3. The fourth Inmarsat-2 was launched in 1992 and is used to provide leased capacity over the Indian Ocean and backing up Inmarsat I-3 F1 and Inmarsat I-3 F3.

Inmarsat-3: A story of spotbeams

Launched in 1996-8, the Inmarsat I-3s were built by Lockheed Martin Astro Space (now Lockheed Martin Missiles & Space) of the USA, responsible for the basic spacecraft, and the European Matra Marconi Space (now Astrium), which developed the communications payload.

The Inmarsat I-3 communications payload can generate a global beam and a maximum of seven spot-beams. The spotbeams are directed as required to make extra communications capacity available in areas where demand from users is high.

Inmarsat I-3 F1 was launched in 1996 to cover the Indian Ocean Region. Over the next two years F2 entered service over Atlantic Ocean Region-East, followed by F3 (Pacific Ocean Region), F4 (Atlantic Ocean Region-West) and F5 (limited services on a single spot beam, back-up and leased capacity).

Inmarsat I-4: Gateway to broadband

Responding to the growing demand from corporate mobile satellite users for high-speed Internet access and multimedia connectivity, Inmarsat has been building its fourth generation of satellites.

The company awarded European spacecraft manufacturer Astrium the contract to build the three Inmarsat I-4 satellites. Astrium is the European company that includes the former Matra Marconi Space, which built the Inmarsat I-2 satellites and the payload for the Inmarsat I-3s.

The job of the satellites will be to support the new Broadband Global Area Network (BGAN), currently scheduled to enter service in 2005 to deliver Internet and intranet content and solutions, video-on-demand, videoconferencing, fax, e-mail, phone and LAN access at speeds up to 432 kbit/s almost anywhere in the world. BGAN will also be compatible with third-generation (3G) cellular systems.

The satellites, the world’s largest commercial communications satellites, will be 100 times more powerful than the present generation and BGAN will provide at least 10 times as much communications capacity as today’s Inmarsat network.

The spacecraft will be built largely in the United Kingdom. The bus will be assembled at Astrium’s factory in Stevenage and the payload in Portsmouth. The two sections will then be united in Toulouse, France, together with the US-built antenna and German-built solar arrays.

Inmarsat maritime communications and safety services contribute significantly to the safe and efficient management of ocean-going vessels whether merchant, fishing or leisure and luxury yachts.

Fleet services

Fleet F77, F55 and F33 provide high-quality mobile voice and flexible data communications services, e-mail and secure Internet access for the maritime industry.

Fleet F77

Inmarsat Fleet F77 is a successor to the Inmarsat B service for deep-sea vessels. In addition to voice and fax, Fleet F77 provides both Mobile ISDN and the Mobile Packet Data Service (MPDS).

The 128 kbit/s ISDN channel enables large volumes of data to be transferred cost-effectively, and remote diagnostics to be carried out.

MPDS brings always-on connectivity to the bridge, with fully integrated Internet Protocol (IP) functionality. Operators are charged by the volume transferred, not for the time spent online, making it a cost-effective service for a range of applications. Officers and crew can access the Internet and browse the web, providing them with education, entertainment and information services.

Inmarsat Fleet F77 also meets the latest distress and safety requirements as specified by the International Maritime Organization (IMO) in resolution A.888 for voice pre-emption and prioritization within the Global Maritime Distress and Safety System (GMDSS).

> *Applications:* data transfer; Internet; LAN and private network access; e-mail; fax; instant messaging; SMS; voice; crew calling; encryption; video-conferencing; store-and-forward video; remote monitoring; chart and weather updates; telemedicine; GMDSS.

Fleet F55

Fleet F55 uses a medium-sized antenna for smaller vessels, and offers the 64 kbit/s Mobile ISDN and MPDS capabilities in the spotbeam areas, plus global voice. Smaller vessels, like trawlers and yachts, are not required to meet IMO regulations, so Fleet F55 and F33 do not include a GMDSS component.

> *Applications:* data transfer; Internet; LAN and private network access; e-mail; fax; instant messaging; SMS; voice; crew calling; encryption; videoconferencing; store-and-forward video; remote monitoring; chart and weather updates; telemedicine.

Fleet F33

F33 offers global telephone, as well as the Mobile Packet Data Service (MPDS) and enhanced 9.6 kbit/s data and fax services within the Inmarsat spotbeams, providing a wide range of applications to the small vessel market.

> *Applications:* data transfer; Internet; LAN and private network access; e-mail; fax; instant messaging; SMS; voice; crew calling; encryption; store-and-forward video; remote monitoring; chart and weather updates; telemedicine.

Inmarsat mini-M

Inmarsat mini-M provides voice and 2.4 kbit/s data (or 9.6 kbit/s using compression) within the Inmarsat spotbeams. It makes the ideal Crew Calling solution when a payphone or crew extension is connected.

> *Applications:* data transfer; e-mail; fax; voice; crew calling; encryption; telemedicine.

Inmarsat C

A two-way, packet data service via lightweight, low-cost terminals small enough to be fitted to any vessel. Approved for use under the Global Maritime Distress and Safety System (GMDSS), it provides seven of the key GMDSS functions. Inmarsat C is ideal for distributing and collecting information from fleets of commercial vessels. It also meets the requirements for Ship Security Alert Systems (SSAS).

> *Applications:* data transfer; e-mail; SMS, crew calling; telex; remote monitoring; tracking; chart and weather updates; maritime safety information (MSI); maritime security; GMDSS; and SafetyNET and FleetNET services.

Inmarsat mini-C

Inmarsat mini-C offers the same primary functions as Inmarsat C through a lower-power, more cost-effective terminal. It is also GMDSS compatible and meets the requirements for Ship Security Alert Systems (SSAS).

> *Applications:* data transfer; e-mail; SMS, remote monitoring; and tracking; maritime security.

Inmarsat D+

A two-way data communications service from equipment the size of a personal CD player. With an integral GPS, Inmarsat D+ can be used for remote surveillance, asset tracking and short information broadcasts. It meets the requirements for Ship Security Alert Systems (SSAS).

> *Applications:* data transfer; remote monitoring; tracking.

Inmarsat E/E+

The Inmarsat E emergency position indicating radio beacon (EPIRB) is a key element of GMDSS. Distress alerts are transmitted from the EPIRB when the unit floats free from a sinking vessel, or when activated manually, and are forwarded automatically to a Maritime Rescue Coordination Centre. Inmarsat E+ adds a key return channel to the EPIRB, which sends a confirmation to the seafarer that their alert has been received.

> *Applications:* GMDSS.

Inmarsat A

The Inmarsat A system provides two-way direct-dial phone connection, including high-quality voice, fax, telex, e-mail and data communications to and from anywhere in the world with the exception of the poles. It also provides distress communication capabilities. It is based on analogue technology and supports data rates of between 9.6 kbit/s up to 64 kbit/s depending on different elements of the end-to-end connection.

> *Applications:* voice; fax; telex; e-mail; data; GMDSS.

Inmarsat B

This remains a core service for the maritime industry. Voice, data at speeds from 9.6 kbit/s to 64 kbit/s, telex and fax are supported, in addition to voice, distress and safety.

> *Applications:* data transfer; Internet; LAN and private network access; e-mail; fax; SMS; voice; crew calling; encryption; video-conferencing; store-and-forward video; remote monitoring; chart and weather updates; telemedicine; GMDSS.

Inmarsat M

Provides global voice and 2.4 kbit/s data on a medium-sized antenna.

> *Applications:* data transfer; fax; voice.

Airtime services for Inmarsat satellites are available worldwide through a network of about 100 service providers. Some service providers also operate Inmarsat land earth stations. There are about 40 such stations in 31 countries. These stations receive and transmit communications through the Inmarsat satellites and provide the connection between the satellite system and the fixed communications networks.

2.5.2.2 VSAT

Very Small Aperture Terminal (VSAT) is a satellite communications technology using small earth antenna, usually 0.9 and 1.8 metres in diameter, for reliable voice, data, audio, video, multimedia, and wideband service transmission. VSAT services constitute a network composed of a series of remote points connected to a main control centre, which in turn is connected through space with a data centre or central processor: the central station and a large number of geographically disbursed sites. One of the many applications of this technology is Internet via satellite.

VSAT communication networks are comprised of a space and a land segment. The space segment is comprised of a geostationary satellite, which amplifies and changes frequencies. The land component consists of a central station or *hub* and remote VSAT stations. VSAT networks can be configured in star-like or mesh shapes, based on the normal flow of communications through the hub or can be sent directly between the VSAT stations (with no need for double hopping).

Changes in technology have led to a reduction in antenna size and have decreased the cost and size of electronics, increased bandwidths and permitted better management capabilities.

When the communication requirement is to provide a long distance link between two or more nodes of a fixed network, a user may select VSAT for such full time, guaranteed bandwidth. For example, some Internet service providers in South America and Africa connect their router to the main Internet by a VSAT full time high-speed link.

VSAT can provide a single communications platform capable of providing service to an entire country or region. For semi-permanent or permanent applications with a large volume of traffic, VSAT may prove to be the best option for telecommunications service.

For VSAT terminals, set-up time varies from 30 minutes to 3 hours, depending on system complexity.

2.5.2.3 USAT networks

The diffusion of VSAT networks in fixed-satellite service (FSS) with small-antenna earth stations at distant locations – such as the terraces of office buildings, hotels, shopping centres and other useful locations – has stimulated the development of antennas that are even smaller than VSATs, generally with an effective aperture of less than 1 m. In general, they are known as Ultra Small Aperture Terminals (USATs). Antenna discrimination naturally deteriorates as its size decreases.

Satellite service provides wide-band and direct access to the backbone of the Internet for reception and/or reception-transmission of Internet information. Point-to-multipoint connections using high-speed frame relay technology are used. Standard Single Channel Per Carrier (SCPC) satellite connections can also be used. Or both systems can be used for the purposes of redundancy.

3 Methods of radiocommunication

3.1 Frequencies

Radio frequencies should be selected according to propagation requirements, allocation to the service for which they are used and in accordance with licensing regulations of the country in which the station is operating.

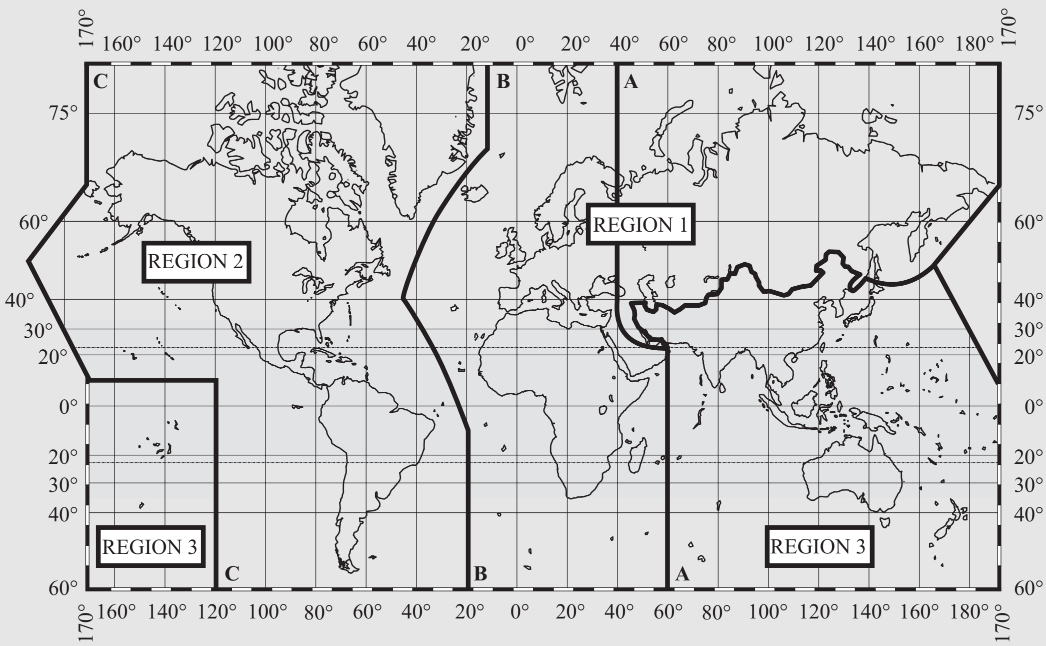
Example 1: An amateur station licensed to operate in the country may use a frequency of 7 050 kHz to communicate via sky wave with a station 300 km away, as this frequency is within the 7 MHz amateur allocation.

Example 2: A land mobile station licensed to operate in a country and assigned an operating frequency of 151.25 MHz may use this frequency to communicate up to about 60 km with other authorised stations.

3.1.1 International frequency allocations

The radio frequency spectrum is divided into bands of frequencies by means of international treaty conferences of the International Telecommunication Union (ITU). These bands are allocated to specific radio services and are listed in Article S5 of the international Radio Regulations. Some bands are allocated to the same service(s) worldwide, while others are allocated to different services on a regional basis. The three Regions are shown in the following map.

Figure 4 – ITU radio regions



The shaded part represents the Tropical Zones as defined in Nos. **S5.16** to **S5.20** and **S5.21.**

S5-01

A simplified table of frequencies allocated to the amateur, fixed and mobile services is shown in Table 1.

Table 1 – Allocation to amateur, fixed and mobile services (simplified, footnotes omitted)

Region 1	Region 2	Region 3
1 810-1 850 AMATEUR	**1 800-1 850** AMATEUR	**1 800-2 000** AMATEUR FIXED
1 850-2 000 FIXED MOBILE except aeronautical mobile	**1 850-2 000** AMATEUR FIXED MOBILE except aeronautical mobile	MOBILE except aeronautical mobile
2 000-2 045 FIXED MOBILE except aeronautical mobile (R)	**2 000-2 065** FIXED MOBILE	
2 045-2 160 FIXED MOBILE		
	2 107-2 170 FIXED MOBILE	
2 194-2 300 FIXED MOBILE except aeronautical mobile (R)	**2 194-2 300** FIXED MOBILE	
2 502-2 625 FIXED MOBILE except aeronautical mobile (R)	**2 505-2 850** FIXED MOBILE	
2 650-2 850 FIXED MOBILE except aeronautical mobile (R)		
3 155-3 400	FIXED MOBILE except aeronautical mobile (R)	
3 500-3 800 AMATEUR FIXED MOBILE except aeronautical mobile	**3 500-3 750** AMATEUR	**3 500-3 900** AMATEUR FIXED MOBILE
	3 750-4 000	
3 800-3 900 FIXED LAND MOBILE	AMATEUR FIXED MOBILE except aeronautical mobile (R)	
3 950-4 000 FIXED		**3 950-4 000** FIXED
4 000-4 063	FIXED	
4 438-4 650 FIXED MOBILE except aeronautical mobile (R)		**4 438-4 650** FIXED MOBILE except aeronautical mobile
4 750-4 850 FIXED LAND MOBILE	**4 750-4 850** FIXED MOBILE except aeronautical mobile (R)	**4 750-4 850** FIXED LAND MOBILE
4 850-4 995	FIXED LAND MOBILE	
5 005-5 060	FIXED	
5 060-5 450	FIXED MOBILE except aeronautical mobile	
5 450-5 480 FIXED LAND MOBILE		**5 450-5 480** FIXED LAND MOBILE
5 730-5 900 FIXED MOBILE except aeronautical mobile (R)	**5 730-5 900** FIXED MOBILE except aeronautical mobile (R)	**5 730-5 900** FIXED MOBILE except aeronautical mobile (R)
6 765-7 000	FIXED LAND MOBILE	
7 000-7 100	AMATEUR AMATEUR-SATELLITE	
	7 100-7 300 AMATEUR	
7 350-8 100	FIXED LAND MOBILE	
8 100-8 195	FIXED	
9 040-9 400	FIXED	
9 900-9 995	FIXED	
10 100-10 150	FIXED AMATEUR	
10 150-11 175	FIXED MOBILE except aeronautical mobile (R)	
11 400-11 600	FIXED	

Table 1 (*cont.*)

Region 1	Region 2	Region 3
12 100-12 230	FIXED	
13 360-13 410	FIXED	
13 410-13 570	FIXED MOBILE except aeronautical mobile (R)	
13 870-14 000	FIXED MOBILE except aeronautical mobile (R)	
14 000-14 250	AMATEUR AMATEUR-SATELLITE	
14 250-14 350	AMATEUR	
14 350-14 990	FIXED MOBILE except aeronautical mobile (R)	
15 800-16 360	FIXED	
17 410-17 480	FIXED	
18 030-18 068	FIXED	
18 068-18 168	AMATEUR AMATEUR-SATELLITE	
18 168-18 780	FIXED MOBILE except aeronautical mobile	
19 020-19 680	FIXED	
19 800-19 990	FIXED	
20 010-21 000	FIXED MOBILE	
21 000-21 450	AMATEUR AMATEUR-SATELLITE	
21 850-21 924	FIXED	
22 855-23 000	FIXED	
23 000-23 200	FIXED MOBILE except aeronautical mobile (R)	
23 200-23 350	FIXED	
23 350-24 000	FIXED MOBILE except aeronautical mobile	
24 000-24 890	FIXED LAND MOBILE	
24 890-24 990	AMATEUR AMATEUR-SATELLITE	
25 010-25 070	FIXED MOBILE except aeronautical mobile	
25 210-25 550	FIXED MOBILE except aeronautical mobile	
26 175-27 500	FIXED MOBILE except aeronautical mobile	
27.5-28	FIXED MOBILE	
28-29.7	AMATEUR AMATEUR-SATELLITE	
29.7-47	FIXED MOBILE	
	47-50 FIXED MOBILE	**47-50** FIXED MOBILE
	50-54 AMATEUR	
	54-68 FIXED MOBILE	**54-68** FIXED MOBILE
68-74.8 FIXED	**68-72** FIXED MOBILE	**68-74.8** FIXED MOBILE
MOBILE except aeronautical mobile	**72-73** FIXED MOBILE	
	74.6-74.8 FIXED MOBILE	
75.2-87.5 FIXED	**75.2-75.4** FIXED MOBILE	
MOBILE except aeronautical mobile	**75.4-76** FIXED MOBILE	**75.4-87** FIXED MOBILE
	76-88 FIXED MOBILE	
		87-100 FIXED MOB ILE
137-138	FIXED MOBILE except aeronautical mobile (R)	
	138-144 FIXED MOBILE	**138-144** FIXED MOBILE
144-146	AMATEUR AMATEUR-SATELLITE	
146-148 FIXED MOBILE except aeronautical mobile (R)	**146-148** AMATEUR	**146-148** AMATEUR FIXED MOBILE
148-149.9 FIXED MOBILE except aeronautical mobile (R)	**148-149.9** FIXED MOBILE	

Table 1 *(end)*

Region 1	Region 2	Region 3
150.05-174 FIXED MOBILE except aeronautical mobile	**150.05-174** FIXED MOBILE	
	174-216 FIXED MOBILE	**174-223** FIXED MOBILE
	216-220 FIXED	
	220-225 AMATEUR	
223-230 FIXED MOBILE	FIXED MOBILE	**223-230** FIXED MOBILE
401-406	FIXED Mobile except aeronautical mobile	
406.1-430	FIXED MOBILE except aeronautical mobile	
430-440 AMATEUR	**430-440** Amateur	
440-450	FIXED MOBILE except aeronautical mobile	
450-470	FIXED MOBILE	

3.1.2 National frequency allocations

The frequency allocation tables of most countries closely follow the international table of allocations. There are exceptions and it is necessary to be aware of, and adhere to, national radio regulations concerning frequencies and their use.

3.1.3 Frequency assignments

Assignment of specific radio frequencies to radio stations is made by national administrations. This is the case for the fixed and mobile services. Amateur stations do not normally have frequency assignments and are free to select a specific operating frequency dynamically within an allocated band.

In some cases, administrations may assign frequencies to services not allocated to those services in the international table of allocations on a non-interference basis. This is provided for in the Radio Regulations, as follows:

- **S4.4** Administrations of the Member States shall not assign to a station any frequency in derogation of either the Table of Frequency Allocations in this Chapter or the other provisions of these Regulations, except on the express condition that such a station, when using such a frequency assignment, shall not cause harmful interference to, and shall not claim protection from harmful interference caused by, a station operating in accordance with the provisions of the Constitution, the Convention and these Regulations.

In times of emergency, administrations may use the following provision of the Radio Regulations:

- **S4.9** No provision of these Regulations prevents the use by a station in distress, or by a station providing assistance to it, of any means of radiocommunication at its disposal to attract attention, make known the condition and location of the station in distress, and obtain or provide assistance.

Stations in the fixed and mobile services having emergency communications missions should have a family of frequencies from which to select according to propagation for specific paths.

3.2 Propagation

Radio signals are electromagnetic waves that travel through the Earth's atmosphere and into space. These waves propagate by means of difference mechanisms, such as surface wave, direct or space wave (line-of-sight), diffraction (knife-edge propagation), ionospheric refraction (sky wave), tropospheric refraction and tropospheric ducting. Ionospheric propagation varies according to time of day, season of the year, solar activity (sunspot number), path distance, and location of the transmitters and receivers. Tropospheric propagation is somewhat related to weather conditions.

Recommendation ITU-R P.1144, the guide to the propagation methods of Radiocommunication Study Group 3, may be used to determine which propagation methods should be used for different applications. Computer programmes are also available and are available from ITU-R.

3.2.1 Ground wave

Ground waves are those confined to the Earth's lower atmosphere. Distances are dependent on transmitter power, antenna efficiency, ground conductivity and atmospheric noise levels. Ground-wave propagation curves for frequencies between 10 kHz and 30 MHz are given in Recommendation ITU-R P.368. For practical emergency communications, ground waves are useful only at lower high frequencies (near 3 MHz) and for relatively short distances of a few kilometres.

3.2.2 Sky wave propagation

Sky waves use the Earth's ionosphere to refract the signal. The ionosphere is formed by several layers, which are identified by letters of the alphabet. The *D layer* lies between about 60 and 92 km above the Earth. The *E layer* is about 100 to 115 km above the Earth. The D layer is used for medium frequency sky wave propagation. The D and E layers absorb signals at frequencies in the lower part of the HF band around 3 MHz. The *F layer* (about 160 to 500 km) may split into two layers, F_1 and F_2 and can support frequencies over the entire HF band at long distances. Frequencies and distances vary according to the specific path, time of day, season and solar activity. Sky wave propagation for the frequency range 2-30 MHz may be predicted using Recommendation ITU-R P.533.

Figure 5 – Illustration of how HF radio signals travel through the ionosphere

Frequencies above the maximum usable frequency (MUF) penetrate the ionosphere and go into space. Frequencies below the MUF are refracted back to the Earth. Ground waves, skip zones and multiple hop paths are shown.

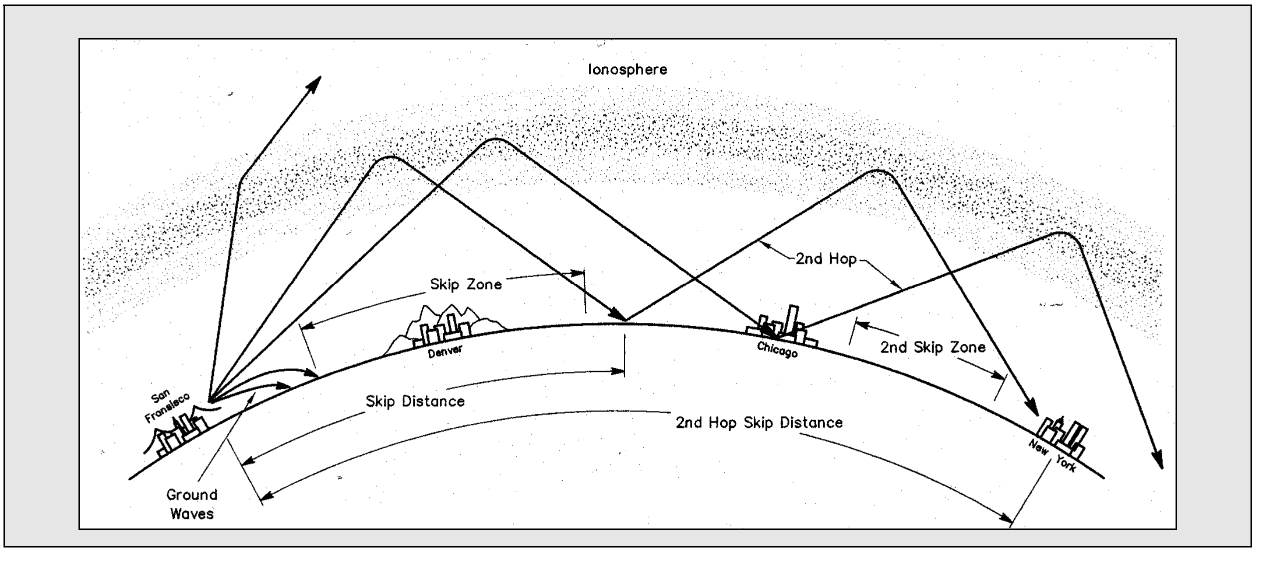


Figure 6 – The ionosphere consists of several regions of ionised particles at different heights above Earth

At night, the D and E regions disappear. The F_1 and F_2 regions combine to form a single F region at night.

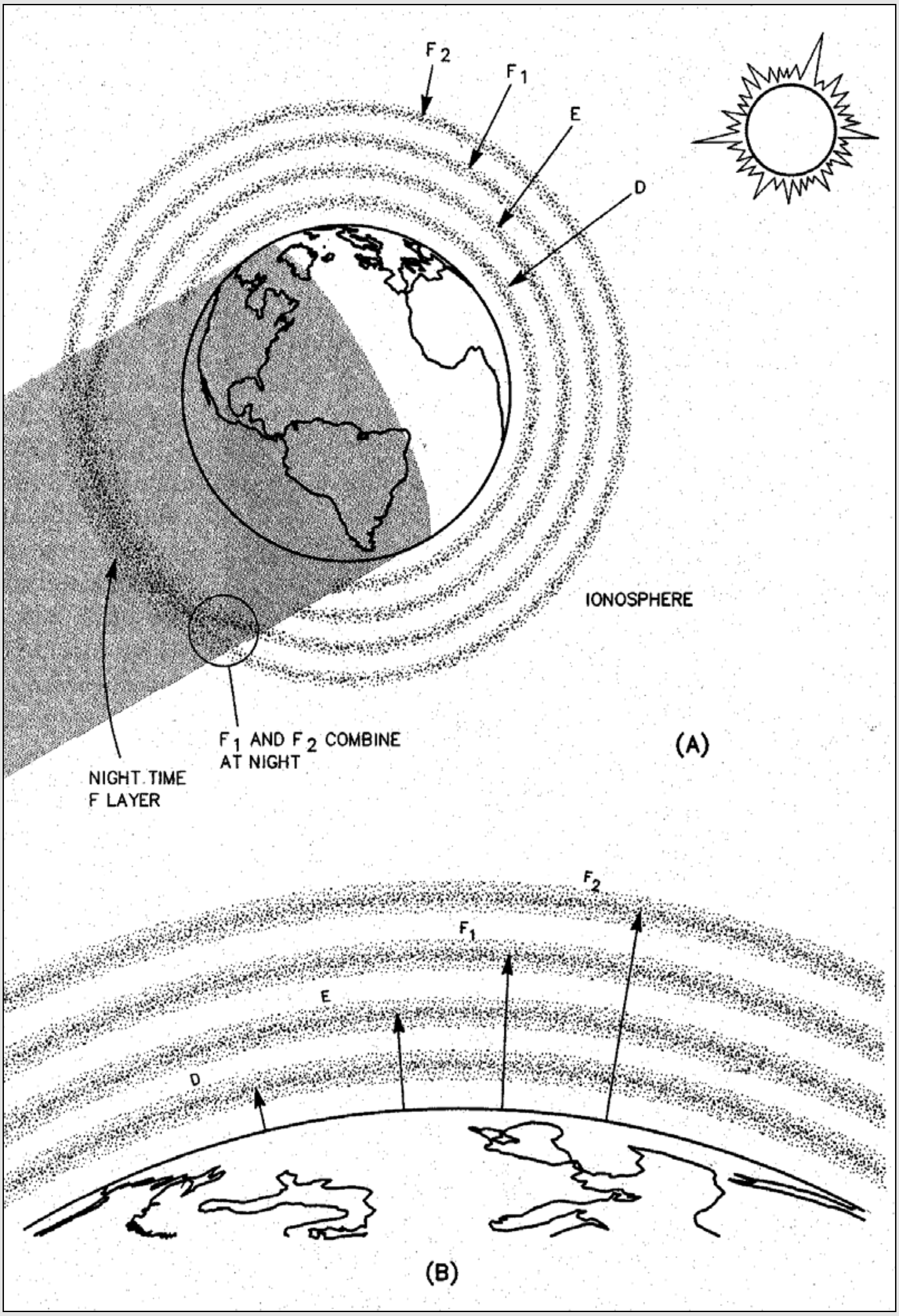
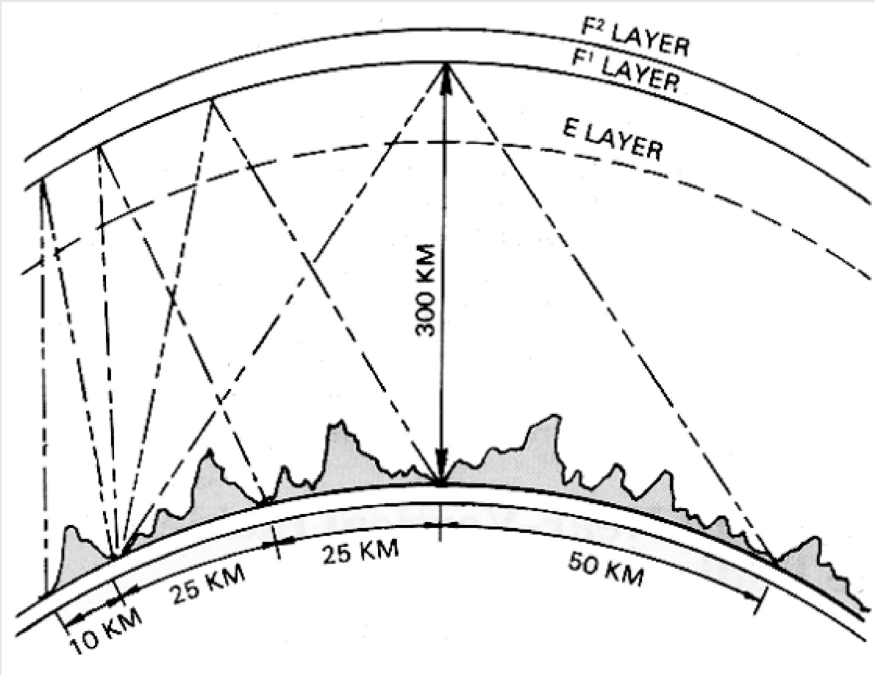


Figure 7 – Near-vertical incidence sky wave paths



3.2.2.1 Near-vertical-incidence sky wave

Near-vertical-incidence sky wave (NVIS) is a term describing high angle ionospheric paths covering short distances. It is particularly useful for distances just beyond those practical for VHF or UHF. To be successful, it is necessary to select frequencies below the critical frequency, which means that frequencies will be in the 2-6 MHz range, the higher end during the daytime and the lower part of the range at night. Antenna take-off angle is essentially straight overhead so a practical antenna is horizontally polarised and just a few metres above ground.

3.2.3 VHF/UHF propagation

Radio signals travel somewhat beyond the optical line-of-sight, as though the Earth were 4/3 its size. The radio horizon for VHF/UHF signals can be approximated by:

$$D = 4.124\ h^{-2}$$

where:

D: distance in kilometres,

h^{-2}: square root of the antenna height above ground in metres.

Free-space propagation loss may be calculated using Recommendation ITU-R P.525.

3.2.3.1 Point-to-area links

If there is a transmitter serving several randomly distributed receivers (for example in the mobile service), the field is calculated at a point located at some appropriate distance from the transmitter by the expression:

$$e = \frac{\sqrt{30p}}{d}$$

where:

e: r.m.s. field strength (V/m) (see Note 1),

p: equivalent isotropically radiated power (e.i.r.p.) of the transmitter in the direction of the point in question (W),

d: distance from the transmitter to the point in question (m).

Land mobile point-to-area propagation for the VHF (10-600 km) and UHF (1-100 km) may be predicted using Recommendation ITU-R P.529.

3.2.3.2 Point-to-point links

With a point-to-point link it is preferable to calculate the free-space attenuation between isotropic antennas, also known as the free-space basic transmission loss (symbols: L_{bf} or A_0), as follows:

$$L_{bf} = 20 \log \left(\frac{4\pi d}{\lambda} \right) \quad \text{dB}$$

where:

L_{bf}: free-space basic transmission loss (dB),

d: distance,

λ: wavelength, and

d and λ are expressed in the same unit.

The above equation can also be written using the frequency instead of the wavelength.

$$L_{bf} = 32.4 + 20 \log f + 20 \log d \quad \text{dB}$$

where:

f: frequency (MHz),

d: distance (km).

Point-to-area propagation for 150 MHz – 40 GHz for distances up to 200 km may be predicted using Recommendation ITU-R P.530.

3.2.3.3 Conversion formulas

On the basis of free-space propagation, the following conversion formulas may be used.

Field strength for a given isotropically transmitted power:

$$E = P_t - 20 \log d + 74.8$$

Isotropically received power for a given field strength:

$$P_r = E - 20 \log f - 167.2$$

Free-space basic transmission loss for a given isotropically transmitted power and field strength:

$$L_{bf} = P_t - E + 20 \log f + 167.2$$

Power flux-density for a given field strength:

$$S = E - 145.8$$

where:

- P_t: isotropically transmitted power (dB(W))
- r: isotropically received power (dB(W))
- E: electric field strength (dB(μV/m))
- f: frequency (GHz)
- d: radio path length (km)
- L_{bf}: free-space basic transmission loss (dB)
- S: power flux-density (dB(W/m^2)).

For further information on point-to-point line-of-sight propagation refer to Recommendation ITU-R P. 530.

4 Antennas as an essential part of any radio station

4.1 Choosing an antenna

Communicators quickly learn two antenna truths:

- Any antenna is better than no antenna.
- Time, effort and money invested in the antenna system generally will provide more improvement to communications than an equal investment to any other part of the station.

The antenna converts electrical energy to radio waves and radio waves to electrical energy, which makes two-way radio communication possible with just one antenna.

Success in communicating depends heavily on an antenna. A good antenna can make a fair receiver perform well. It can also make a few watts sound like much more. Since the same antenna is used to transmit and receive, any improvements to the antenna make the signal stronger at the desired reception points. Some antennas work better than others. It is useful to experiment with different antenna types.

4.2 Antenna system considerations

4.2.1 Safety

Safety should be the first consideration in installing an antenna system.

An antenna or transmission line should never be installed on top of electrical power lines. A vertical antenna should never be located where it could fall against the electrical power lines. Electrocution could result if power lines ever come into contact with the antenna.

Antennas should be high enough above the ground to ensure that no one can touch them. When the transmitter is active, the high voltages present at the ends of an antenna could kill or at least cause a serious RF burn.

A lightning arrester should be placed on the transmission line at the entrance point to the building housing the transmitting and receiving equipment. For safety, an Earth ground connection is necessary and the wire used for that purpose should be of conductor size equivalent to at least 2.75 mm diameter wire. The heavy aluminium wire used for TV-antenna Earth grounds is satisfactory. Copper braid 20 mm wide is also suitable. Ground connection may be made to a metal water pipe system, the grounded metal frame of a building, or to one or more 15 mm diameter ground rods driven to a depth of at least 2.5 metres.

Antenna work sometimes requires that someone climb up on a tower, into a tree, or onto the roof. It is not safe to work alone. Each move should be planned beforehand. The person on a ladder, tower, tree or rooftop should always wear a safety belt and keep it securely anchored. Before each use, the safety belt should be inspected carefully for damage such as cuts or worn areas. The belt will make it much easier to work on the antenna and will also prevent an accidental fall. A hard hat and safety glasses are also important safety equipment.

Tools should not be carried by hand when climbing. They should be placed on a tool belt. A long rope leading back to the ground should be secured to the belt and can be used to pull up other needed objects. It is helpful (and safe) to tie strings or lightweight ropes to all tools. This will save time in retrieving dropped tools and reduce the chances of injuring a helper on the ground.

Helpers on the ground should never stand directly under the work being done. All ground helpers should wear hard hats and safety glasses for protection. Even a small tool can cause an injury if it falls from 15 or 20 metres. A helper should always observe the tower work carefully. If possible, an observer with no other duties other than to watch for potential hazards should be positioned with a good view of the work area.

4.2.2 Antenna location

After assembling the antenna components, select a good place for it to be installed. Avoid running the antenna parallel close to power lines or telephone lines. Otherwise unwanted electrical coupling may occur, which could result in either power line noise in the station receiver or the transmitted signal appearing on the power or telephone lines. Avoid running the antenna close to metal objects, such as rain gutters, metal beams, metal siding, or even electrical wiring in the attic of a building. Metal objects may shield the antenna or modify its radiation pattern.

4.2.3 Antenna polarisation

Polarisation refers to the electrical-field characteristic of a radio wave. An antenna that is parallel to the earth’s surface produces horizontally polarised radio waves. One that is perpendicular (at a 90° angle) to the Earth’s surface produces vertically polarised waves.

Polarisation is most important when installing antennas for VHF or UHF. The polarisation of a terrestrial VHF or UHF signal tends not to change from transmitting antenna to receiving antenna. Both transmitting and receiving stations should use the same polarisation. Vertical polarisation is commonly used for VHF and UHF mobile operation including hand-held transceivers, in vehicles and base stations.

For HF sky-wave communications, radio signals tend to rotate through the ionosphere, thus horizontally or vertically polarised antennas can be used with almost equal results. Horizontally polarised antennas are preferred for receiving as they tend to reject local manmade noise, which is usually vertically polarised.

Vertical antennas provide low-angle radiation but have a null (radiate no energy) upward. This makes them suitable for longer sky-wave paths requiring a low take-off angle and they are not recommended for near-vertical-incidence sky-wave (NVIS) paths of about 0-500 km.

4.2.4 Tuning the antenna

The antenna length given by an equation is just an approximation. Nearby trees, buildings or large metal objects and height above ground all affect the resonant frequency of an antenna. An SWR metre can help to determine if the antenna should be shortened or lengthened. The correct length provides the best impedance match for the transmitter.

After cutting the wire to the length given by the equation, the tuning of the antenna should be adjusted for the best operation. With the antenna in its final location, the SWR should be observed at various frequencies within the desired band. If the SWR is much higher at the low-frequency end of the band the antenna is too short. If the antenna is too short, an extra length of wire can be attached to each end with an alligator clip. Then the extra length can be shortened a little at a time until the correct length is reached. If the SWR is much higher at the high-frequency end of the band, the antenna is too long. When the antenna is properly tuned, the lowest SWR values should be around the preferred operating frequency.

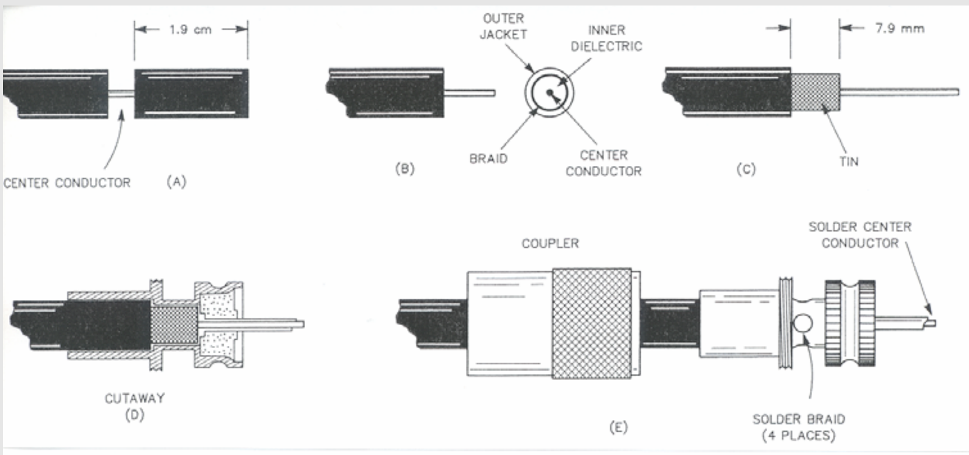
4.2.5 Transmission lines

The most commonly used type of antenna system transmission line is the coaxial cable (“coax”), where one conductor is inside the other. Coaxial cable has several advantages: It is readily available and resistant to weather. It can be buried in the ground if necessary, bent, coiled and run adjacent to metal with little effect.

Most common HF antennas are designed for use with transmission lines having characteristic impedances of about 50 ohms. RG-8, RG-58, RG-174 and RG-213 are commonly used coaxial cables. RG-8 and RG-213 are similar cables, and they have the least loss of the types listed here. The larger coax types (RG-8, RG-213, RG-11) have less signal loss than the smaller types. If the feed line is less than 30 metres long, the small additional signal loss on the HF bands is negligible. On VHF/UHF bands losses are more noticeable, especially when the feed line is long. On these bands, higher-quality RG-213 coax or even lower-loss rigid or semi-rigid coaxial cables minimise losses for transmission lines exceeding 30 metres.

Coaxial cable connectors are an important part of a coaxial feed line. It is prudent to check the coaxial connectors periodically to see that they are clean and tight to minimise any loses. If a bad solder connection is suspected, the joints should be cleaned and re-soldered. The choice of connectors normally depends on matching connectors on the radios. Many HF radios and many VHF radios use SO-239 connectors. The mating connector is a PL-259 (Figure 7). The PL-259 is sometimes called a UHF connector, although constant impedance connectors such as Type-N the best choice for the UHF bands. PL-259 connectors are designed for use with RG-8 or RG-213 cables. When using coax to connect the transmission line, an SO-239 connector should terminate the line at the centre insulator and a PL-259 should be used at the end connecting to the radio.

Figure 8 – PL-259 coaxial connector



4.2.6 Matching impedances within the antenna system

If an antenna system does not match the characteristic impedance of the transmitter, some of the power is reflected back from the antenna to the transmitter. When this happens, the RF voltage and current are not uniform along the line. The power travelling from the transmitter to the antenna is called forward power and is radiated from the antenna. The standing-wave ratio (SWR) is the ratio of the maximum voltage on the line to the minimum voltage. An SWR metre measures the relative impedance match between an antenna and its feed line. Lower SWR values mean a better impedance match exists between the transmitter and the antenna system. If a perfect match exists, the SWR is 1:1. The SWR defines the quality of an antenna as seen from the transmitter, but a low SWR does not guarantee that the antenna will radiate the RF energy supplied to it by the transmitter. An SWR measurement of 2:1 indicates a fairly good impedance match.

4.2.7 SWR metres

The most common SWR metre application is tuning an antenna to resonate on a given frequency. An SWR reading of 2:1 or less is quite acceptable. A reading of 4:1 or more is unacceptable. This means there is a serious impedance mismatch between the transmitter, the antenna or the feed line.

How the SWR is measured depends on the type of metre. Some SWR metres have a SENSITIVITY control and a FORWARD-REFLECTED switch. If so, the metre scale usually provides a direct SWR reading. To use the metre, first put the switch in the FORWARD position. Then adjust the SENSITIVITY control and the transmitter power output until the metre reads full scale. Some metres have a mark on the metre face labelled SET or CAL. The metre pointer should rest on this mark. Next, set the selector switch to the REFLECTED position. This should be done without readjusting the transmitter power or the metre SENSITIVITY control. Now the metre pointer displays the SWR value. Find the resonant frequency of an antenna by connecting the metre between the feed line and your antenna. This technique will measure the relative impedance match between the antenna and its feed line. The settings that provide the lowest SWR at the operating frequency are preferred.

4.2.8 Antenna impedance matching networks

Another useful accessory is an impedance matching network. It is also called an antenna matching network, antenna tuner, antenna tuning unit (ATU), or simply a tuner. The network compensates for any impedance mismatch between the transmitter, the transmission line and the antenna. A tuner makes it possible to use one antenna on several frequency bands. The tuner is connected between the antenna and SWR metre, if used. The SWR metre is used to indicate the minimum reflected power as the tuner is adjusted.

Just one more step and the antenna installation is complete. After routing the coaxial cable to your station, cut it to length and install the proper connector for the transmitter. Usually this connector will be a PL-259, sometimes called a UHF connector. Figure 7 shows how to attach one of these fittings to RG-8 or RG-11 cable. It is important to place the coupling ring on the cable *before* installing the connector body. If using RG-58 or RG-59 cable, use an adapter to fit the cable to the connector. The SO-239 female connector is standard on many transmitters and receivers.

If the SWR is very high, a problem may exist that cannot be cured by simple tuning. A very high SWR may mean that the feed line is open or shorted. If the SWR is very high the cause may be an improper connection or insufficient space between the antenna and surrounding objects.

4.3 Practical antennas

4.3.1 The half-wave dipole antenna

Probably the most common HF antenna is a wire cut to a half wavelength (½ λ) at the operating frequency. The transmission line attaches across an insulator at the centre of the wire. This is the half-wave dipole. This is often referred to as a dipole antenna. (*Di* means two, so a dipole has two equal parts. A dipole could be a length other than ½ λ.) The total length of a half-wavelength dipole is ½ λ. The feed line connects to the centre. This means that each side of this dipole is ¼ λ long.

Wavelength in space can be determined by dividing the constant 300 by the frequency in megahertz (MHz). For example, at 15 MHz, the wavelength is 300/15 = 20 metres.

Radio signals travel slower in wire than in air, thus the following equation may be used to find the total length of a ½ λ dipole for a specific frequency. Notice that the frequency is given in megahertz and the antenna length is in metres for this equation:

$$\text{L (in metres)} = \frac{143}{f_{\text{MHz}}}$$

This equation also takes into account other factors, often called *antenna effects*. It gives the approximate length of wire for an HF dipole antenna. The equation will not be as accurate for VHF/UHF antennas. The element diameter is a larger percentage of the wavelength at VHF and higher frequencies. Other effects, such as *end effects* also make the equation less accurate at VHF and UHF.

Table 2 – Approximate lengths for ½ λ dipoles suitable for fixed, mobile and amateur bands

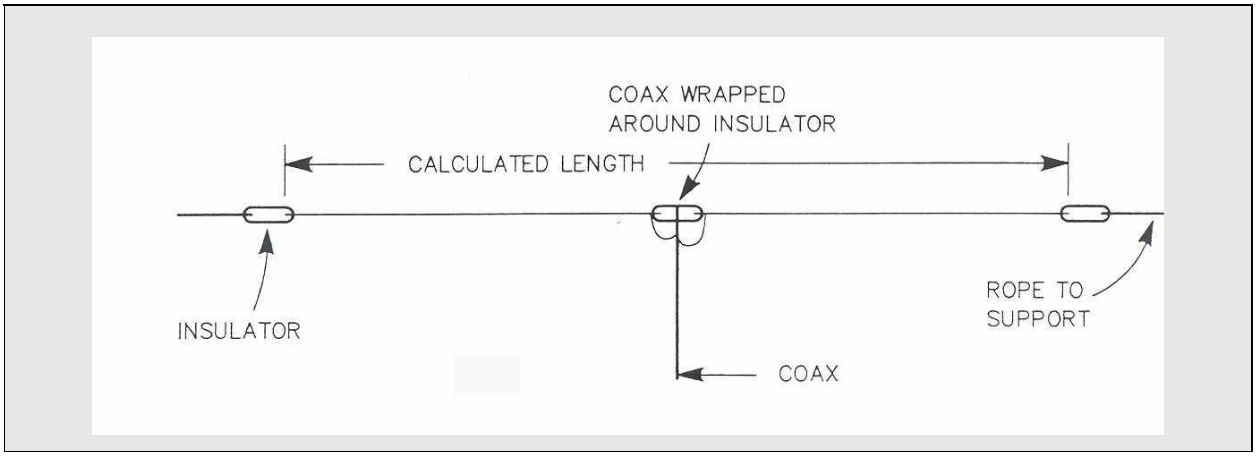
Frequency (MHz)	Length (m)
3.3	43.3
3.5	40.8
3.8	37.6
4.5	31.8
4.9	29.2
5.2	27.5
5.8	24.6
6.8	21.0
7.1	20.1
7.7	18.6
9.2	15.5
9.9	14.4
10.1	14.1
10.6	13.5
11.5	12.4

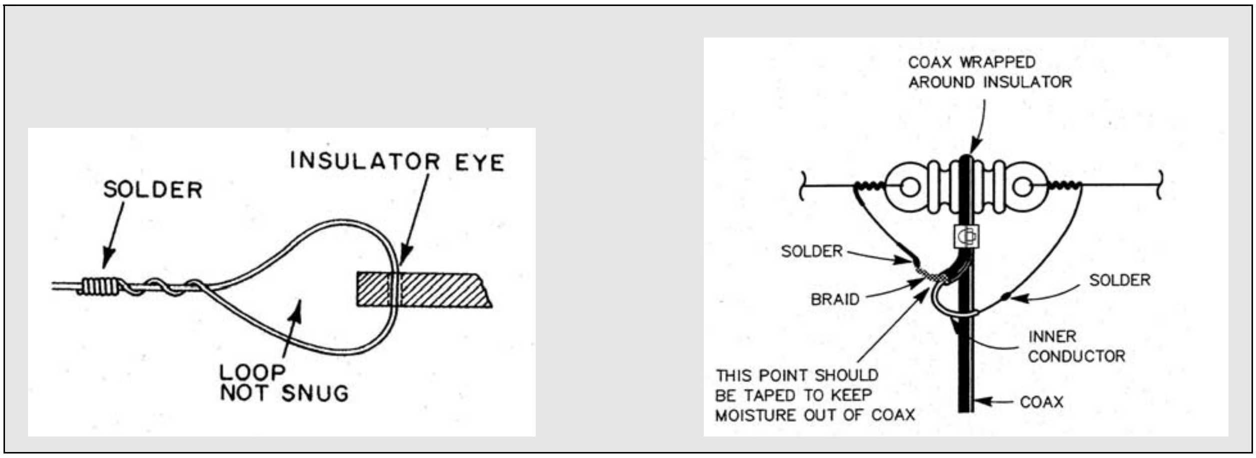
Frequency (MHz)	Length (m)
12.2	11.7
13.4	10.7
13.9	10.3
14.2	10.0
14.6	9.8
16.0	8.8
17.4	8.2
18.1	7.9
20.0	7.1
21.2	6.7
21.8	6.5
23.8	6.0
24.9	5.7
25.3	5.6
29.0	4.9

Frequency (MHz)	Length (m)
30	4.8
35	4.1
40	3.6
50	2.86
145	99 cm
150	95
155	92
160	89
165	87
170	84
435	33
450	32
455	31.4
460	31
465	30.7

Figure 9 – Construction of a simple half-wave dipole antenna

At top is the basic dipole assembly. Bottom left shows how to connect wire ends to insulators. Bottom right illustrates connection of the transmission line to the centre of the dipole.



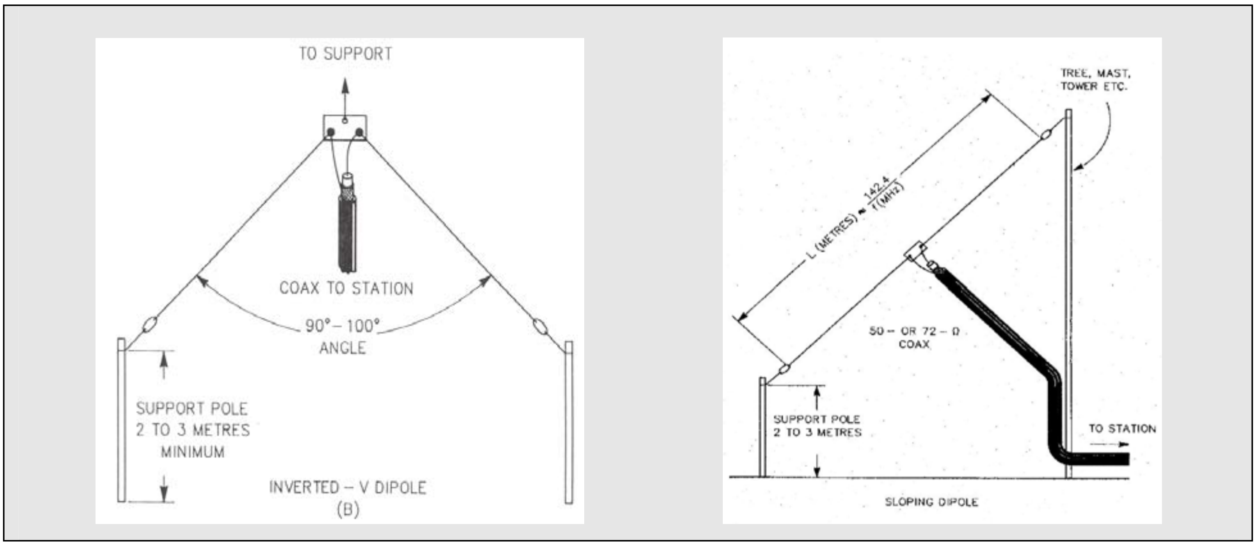


Household electrical wire and stranded wire will stretch with time; a heavy gauge copper-clad steel wire does not stretch as much. The dipole should be cut according to the dimension found by the equation above (total length of a ½ λ dipole), but a little extra length should be provided to wrap the ends around the insulators. A coaxial or parallel transmission line is needed to connect the antenna to the transmitter. Three insulators are also needed. If supporting the antenna in the middle, both ends will droop toward the ground. This antenna, known as an inverted-V dipole, is almost omni-directional and works best when the angle between the wires is equal to or greater than 90°. A dipole can also be supported only at one end, in which case it is known as a sloping dipole.

Dipole antennas radiate best in a direction that is 90° to the antenna wire. For example, suppose a dipole antenna is installed so the ends of the wire run in an east/west direction. Assuming it was sufficiently above the ground (for example, ½ λ high), this antenna would send stronger signals in north and south directions. A dipole also sends radio energy straight up and straight down. Of course, the dipole also emits some energy in directions off the ends of the wire, but these signals will be attenuated. Though it is possible to contact stations to the east and west with this antenna, signals are stronger with stations to the north and south.

Figure 10 – Alternative ways of installing a dipole

The configuration on the left is an Inverted-V dipole. A sloping dipole is shown at right. A balun (not shown) may be used at the feed point, as this is a balanced antenna.



4.3.2 Aeronautical public correspondence stations

A broadband version of the dipole, the folded dipole has an impedance of about 300 ohms and can be fed directly with any length of 300 ohm feed line. This variation of the dipole is termed *broadband* because it offers a better match to the feeder over a somewhat wider range of frequencies. When a folded dipole is installed as an inverted "V" it is essentially omni-directional. There are several broadband folded dipoles available commercially that provide acceptable HF performance, even when operating without a tuner.

4.3.3 Quarter-wavelength vertical antenna

The quarter-wavelength vertical antenna is effective and easy to build. It requires only one element and one support. On the HF bands it is often used for long distance communications. Vertical antennas are referred to as non-directional or omni-directional antennas because they send radio energy equally well in all compass directions. They also tend to concentrate the signals toward the horizon as they have a low-angle radiation pattern and do not generally radiate strong signals upward.

Figure 11 shows how to construct a simple vertical antenna. This vertical antenna has a radiator that is ¼ λ long. Use the following equation to find the approximate length for the radiator. The frequency is given in megahertz and the length is in metres in this equation.

$$L \text{ (in metres)} = \frac{71}{f_{MHz}}$$

Figure 11 – Simple quarter-wave vertical antenna

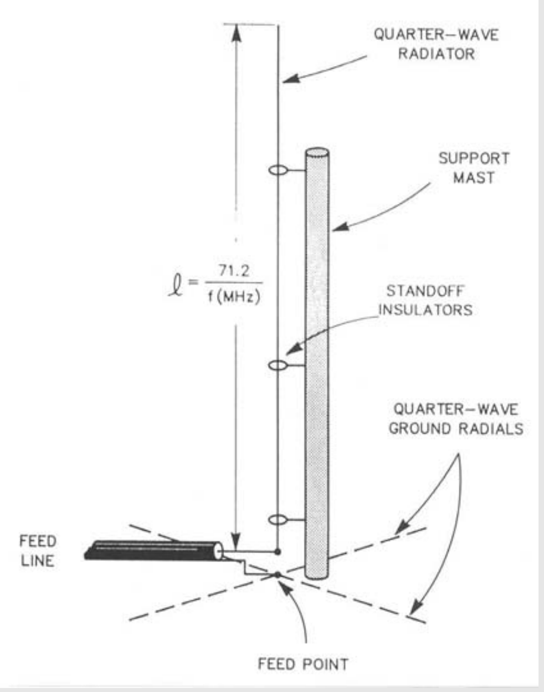


Table 3 – Approximate lengths for ¼ λ monopoles and ground radials suitable for fixed, mobile and amateur bands

Frequency (MHz)	Length (m)
3.3	21.6
3.5	20.4
3.8	18.8
4.5	15.9
4.9	14.6
5.2	13.7
5.8	12.3
6.8	10.5
7.1	10.0
7.7	9.3
9.2	7.7
9.9	7.2
10.1	7.1
10.6	6.7
11.5	6.2

Frequency (MHz)	Length (m)
12.2	5.9
13.4	5.3
13.9	5.1
14.2	5.0
14.6	4.9
16.0	4.5
17.4	4.1
18.1	3.9
20.0	3.5
21.2	3.3
21.8	3.2
23.8	3.0
24.9	2.9
25.3	2.8
29.0	2.5

Frequency (MHz)	Length (m)
30	2.4
35	2.1
40	1.8
50	1.43
145	50 cm
150	48
155	46
160	44
165	43
170	42
435	117
450	16
455	16
460	16
465	15

For successful results, the ¼ λ vertical should have a radial system to reduce Earth losses and to act as a ground plane. For operation on high frequencies, the vertical may be at ground level and the radials placed on the ground. At least 3 radials should be used and out like the spokes of a wheel, with the vertical at the centre. Radials should be at least ¼ λ long or more at the lowest operating frequency.

Most vertical antennas used at HF are ¼ λ long or shorter with appropriate loading networks. For VHF and UHF, antennas are physically short enough that longer verticals may be used. A popular mobile antenna is a 5/8 λ vertical, often called a "five-eighths whip". This antenna is popular because it concentrates more of the radio energy toward the horizon than a ¼ λ vertical.

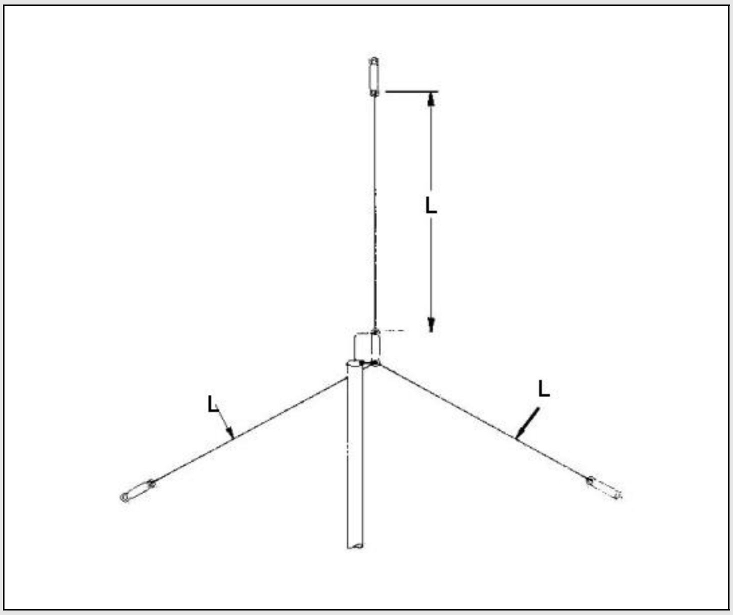
Commercially available vertical antennas need a coax feed line, usually with a PL-259 connector. Just as with the dipole antenna, RG-8, RG-11 or RG-58 coax can be used.

Some manufacturers offer multi-band vertical antennas that use series-tuned circuits (traps) to make the antenna resonant at different frequencies.

To fabricate a tree-mounted HF ground plane antenna (Figure 12), a length of RG-58 cable is connected to the feed point of the antenna and is attached to an insulator. The radial wires are soldered to the coax-line braid at this point. The top of the radiator section is suspended from a tree limb or other convenient support, and in turn supports the rest of the antenna.

Figure 12 – Construction of tree-mounted ground plane antenna

(L = 143/f_{MHz})



The dimensions for the antenna are the same as for a ¼ λ vertical antenna. All three wires of the antenna are ¼ λ long. This generally limits the usefulness of the antenna to 7 MHz and higher bands, as temporary supports higher than 10 or 15 metres may not be available.

4.3.4 Antennas for hand-held transceivers

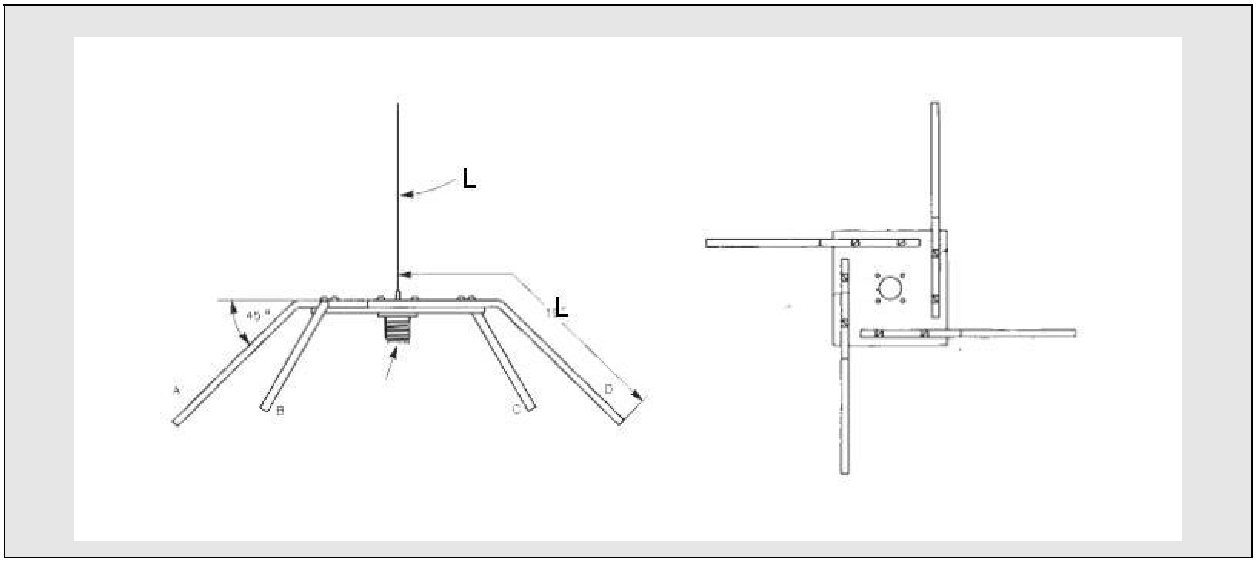
VHF and UHF hand-held transceivers normally use shortened flexible antennas that are inexpensive, small, lightweight and robust. On the other hand, they have some disadvantages: It is a compromise design that is inefficient and thus does not perform as well as larger antennas. Two better-performing antennas are the ¼ λ and the 5/8 λ telescoping types that are available as separate accessories.

4.3.5 Vertical antennas for VHF and UHF

For operation of stations at fixed locations, the ¼ λ vertical is an ideal choice. The 145 MHz model shown in Figure 13 uses a flat piece of sheet aluminium, to which radials are connected with machine screws. A 45° bend is made in each of the radials. This bend can be made with an ordinary bench vise. An SO-239 chassis connector is mounted at the centre of the aluminium plate with the threaded part of the connector facing down. The vertical portion of the antenna is made of 10 mm copper wire soldered directly to the centre pin of the SO-239 connector.

Figure 13 – A VHF or UHF ground plane antenna with 4 drooping radials

($L = 143/f_{MHz}$)



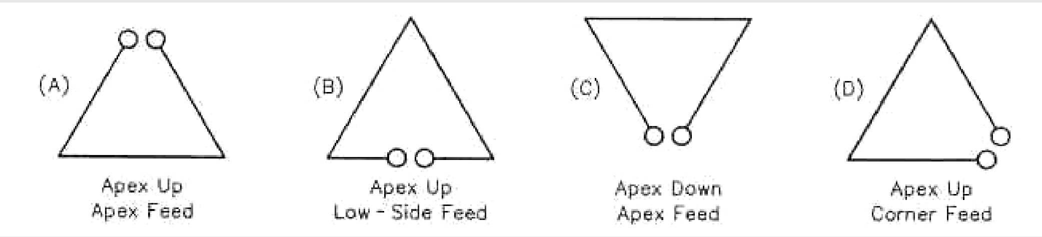
Construction is simple as it requires nothing more than an SO-239 connector and some common hardware. A small loop formed at the inside end of each radial is used to attach the radial directly to the mounting holes of the coaxial connector. After the radial is fastened to the SO-239 with hardware, a large soldering iron or propane torch is used to solder the radial and the mounting hardware to the coaxial connector. The radials are bent to a 45° angle and the vertical portion is soldered to the centre pin to complete the antenna. It is prudent to apply a small amount of sealant around the areas of the centre pin of the connector to prevent the entry of water into the connector and coax line.

4.3.6 Delta loop

The Delta loop is another field expedient wire antenna used by disaster relief organisations. There are three key advantages to a Delta loop antenna: 1) a ground plane is unnecessary; 2) a full-wave loop (depending on the shape) has some gain over a dipole; and 3) a closed loop is a "quieter" (improved signal-to-noise ratio) receiving antenna than are most vertical and some horizontal antennas. Feed point selection will permit the choice of vertical or horizontal polarisation. Various angles of radiation will result from assorted feed-point selections. The system is rather flexible and is capable of maximising close in or long distance communications (high angle versus low angle). Figure 14 illustrates various configurations that can be used. The bandwidth at resonance is similar to a dipole. An antenna-tuning unit (ATU) is recommended for matching the system to the transmitter in parts of the band where the SWR is high. There is no rule that dictates the shape of a full wave loop. It may be convenient to use a triangular shape with the apex is at the top in which case only one high support is needed. Circular, square or rectangular shapes have been used.

Figure 14 – Various configurations for a full-wavelength Delta loop antenna

Overall length of the antenna wire is approximately $286/f_{MHz}$



Configuration	A	B	C	D
Polarisation	Horizontal	Horizontal	Horizontal	Vertical
Radiation angle	Moderately high	High	Moderately high	Low

4.3.7 Directional antennas

Directional antennas have two important advantages over simpler omni-directional antennas such as dipoles and vertical monopoles. As transmitting antennas, they concentrate most of the radiation in one direction. For receiving, directional antennas can be pointed toward the desired direction or away from a source of noise.

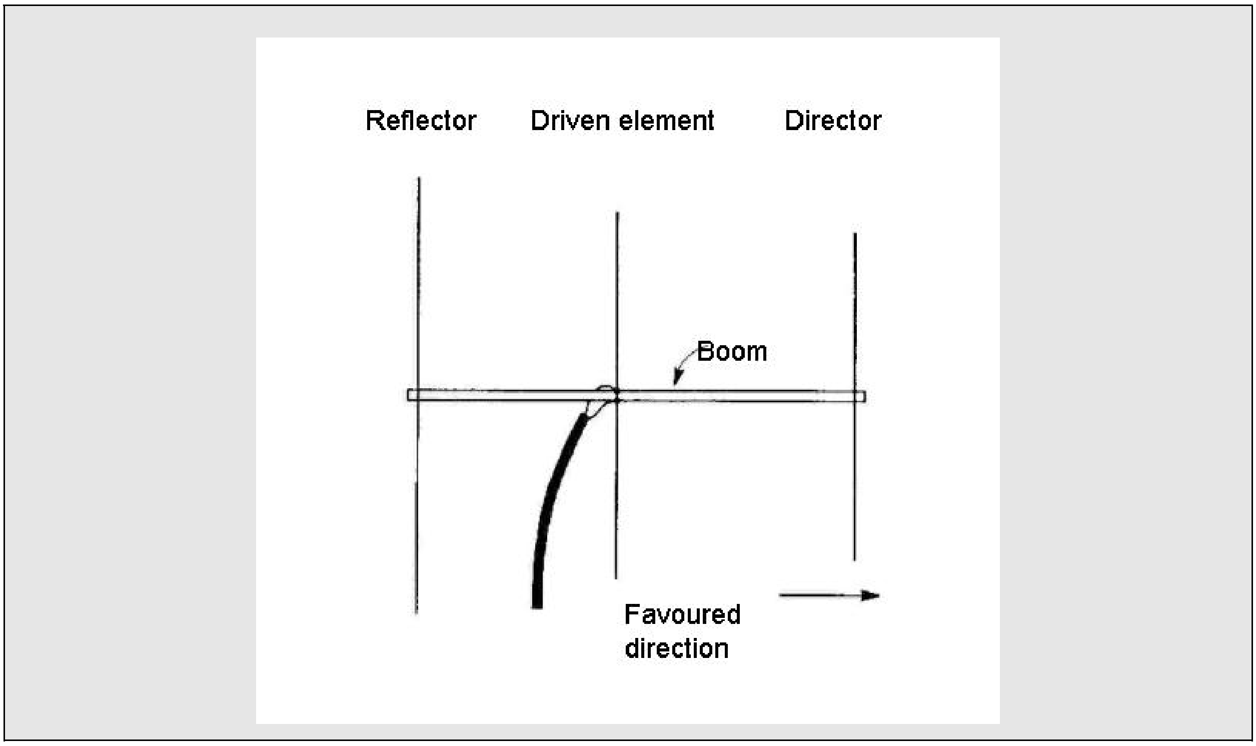
Although generally large and expensive below about 10 MHz, directional antennas often are used on the upper high frequency bands, such as from 10 MHz to 30 MHz. Directional antennas commonly used at VHF and UHF owing to their reasonably small size. The most common directional antenna is the *Yagi* antenna, but there are other types, as well.

A Yagi antenna has several elements attached to a central *boom*, as Figure 15 shows. The elements are parallel to each other and are placed in a straight line along the boom. Although several factors affect the amount of gain of a Yagi antenna, *boom length* has the largest effect: The longer the boom, the higher the gain.

The transmission line connects only to one element called the *driven element*. On a three-element Yagi like the one shown in Figure 15, the driven element is in the middle. The element at the front of the antenna (toward the favoured direction) is a director. Behind the driven element is the reflector element. The driven element is about ½ λ long at the antenna design frequency. The director is a bit shorter than ½ λ, and the reflector a bit longer. Yagi beams can have more than three elements, usually by adding more directors. Directors and reflectors are called parasitic elements, since they are not fed directly.

Communication in different directions may be achieved by turning the array using a rotator in the azimuthal (horizontal) plane, to point it in different directions.

Figure 15 – A three-element Yagi showing the reflector, driven element and director supported by a boom



4.3.7.1 Log-periodic arrays

Log-periodic antennas are an alternative directional antenna. They have wider bandwidth but lower directional gain than a Yagi.

A log-periodic antenna is a system of driven elements, designed for operation over a wide range of frequencies. Its advantage is that it exhibits essentially constant characteristics over the frequency range – the same radiation resistance (and therefore the same SWR), and the same pattern characteristics (approximately the same gain and the same front-to-back ratio).

5 Power sources and batteries

5.1 Power safety

As in antenna work, for safety purposes any electrical work should be done with a second person present. A switch should never be used in the neutral wire without also disconnect the equipment from an active or “hot” line.

All communications equipment should be reliably connected to an Earth ground by means of a separate heavy gauge wire. The power wiring neutral conductor should not be used for this safety ground. This places the chassis of the equipment at Earth ground potential for minimal RF energy on the chassis. It provides a measure of safety for the operator in the event of accidental short or leakage of one side of the power line to the classis.

No battery should be subjected to unnecessary heat, vibration or physical shock. The battery should be kept clean. Frequent inspection of leaks is recommended. Electrolyte that has leaked or sprayed from the battery should be cleaned from all surfaces. The electrolyte is chemically active and electrically conductive, and may ruin electrical equipment. Acid may be neutralized with sodium bicarbonate (baking soda), and alkalis may be neutralized with a weak acid such as vinegar. Both neutralizers will dissolve in water, and should be quickly washed off. The neutralizer should not be allowed to enter the battery. Gas escaping from storage batteries may be explosive. Keep flames or lighted tobacco products away.

When working with generators, keep safety foremost in your mind. Gasoline is a dangerous chemical and there is no scope for carelessness. Fuel should be stored only in the proper containers, well away from the generator and out of the sun. The generator should be turned off and cool before adding new fuel. Gasoline and oil-soaked rags should be disposed of properly. If they are tossed in a pile, they could catch fire by spontaneous combustion. A fire extinguisher should be kept near the generator. Smoking should not be allowed near the generator.

Internal combustion engines produce heat. The larger the engine, the higher the speed, the greater the heat produced. The combination of fuel fumes and engine heat in a small enclosure is dangerous. Generator exhaust fumes can be lethal. Whether gasoline, diesel, natural gas or propane is used, be sure that exhaust fumes are properly vented out of the operating area. Natural ventilation is usually not sufficient to maintain a safe atmosphere. A blower or ventilator fan should be used to bring fresh air from outside, with an exhaust fan installed to expel the heat.

5.2 Mains power

Mains power should be used when available to save any self-generated power systems for backup purposes. Even unreliable mains power can be used to charge batteries.

Electrical service enters buildings in the form of two or more wires to provide 100-130 V or 200-260 V alternating current at 50 or 60 Hz. The circuits may be divided into several branches and protected by circuit breakers or fuses.

A ground fault circuit interrupter (GFCI or GFI) is also desirable to safety reasons, and should be a part of the electrical power wiring if possible.

5.3 Power transformers

Numerous factors should be considered in selecting transformers, such as input and output volt-ampere (VA) ratings, ambient temperature, duty cycle and mechanical design.

In alternating-current equipment, the term "volt-ampere" is often used rather that the term "watt". This is because ac components must handle reactive power as well as real power. The number of volt-amperes delivered by a transformer depends not only upon the dc load requirements, but also upon the type of dc output filter used (capacitor or choke input), and the type of rectifier used (full-wave centre tap or full-wave bridge). With a capacitive-input filter, the heating effect in the secondary is higher because of the high peak-to-average current ration. The volt-amperes handled by the transformer may be several times the power delivered to the load. The primary winding volt-amperes will be somewhat higher because of transformer losses.

A transformer operates by producing a magnetic field in its core and windings. The intensity of this field varies directly with the instantaneous voltage applied to the transformer primary winding. These variations, coupled to the secondary windings, produce the desired output voltage. Since the transformer appears to the source as an inductance in parallel with the (equivalent) load, the primary will appear as a short circuit if dc is applied to it. The unloaded inductance of the primary must be high enough so as not to draw an excess amount of input current at the design line frequency (normally 50 or 60 Hz). This is achieved by providing sufficient turns on the primary and enough magnetic core materials so that the core does not saturate during each half-cycle.

To avoid possibly serious overheating, transformers and other electromagnetic equipment designed for 60 Hz systems must not be used on 50 Hz power systems unless specifically designed to handle the lower frequency.

5.4 Batteries and charging

The availability of solid-state equipment makes it practical to use battery power under portable or emergency conditions. Hand-held transceivers and instruments are obvious applications, but 100 W output transceivers may be practical users of battery power (for example, emergency power for HF transceivers).

Low-power equipment can be powered from two types of batteries. The *primary* battery is intended for one-time use and is then discarded; the *storage* (or *secondary*) battery may be recharged many times.

A battery is a group of chemical cells, usually connected in series to give some desired multiple of the cell voltage. Each assortment of chemicals used in the cell gives a particular nominal voltage. This must be taken into account to make up a particular battery voltage. For example, four 1.5 V carbon-zinc cells make a 6 V battery and six 2 V lead-acid cells make a 12 V battery.

5.4.1 Battery capacity

The common rating of battery capacity is ampere-hours (Ah), the product of discharge current and time. The symbol *C* is commonly used; C/10, for example, would be the current available for 10 hours continuously. The value of C changes with the discharge rate and might be 110 at 2 A but only 80 at 20 A. Capacity may vary from 35 mAh for some of the small hearing aid batteries to more than 100 Ah for a size 28 deep-cycle storage battery.

Sealed primary cells usually benefit from intermittent (rather than continuous) use. The resting period allows completion of chemical reactions needed to dispose of by-products of the discharge.

The output voltage of all batteries drops as they discharge. “Discharged” condition for a 12 V lead-acid battery, for instance, should not be less than 10.5 V. It is also good to keep a running record of hydrometer readings, but the conventional readings of 1 265 charged and 1 100 discharged apply only to a long, low-rate discharge. Heavy loads may discharge the battery with little reduction in the hydrometer reading.

Batteries that become cold have less of their charge available, and some attempt to keep a battery warm before use is worthwhile. A battery may lose 70% or more of its capacity at cold extremes, but it will recover with warmth. All batteries have some tendency to freeze, but those with full charges are less susceptible. A fully charged lead-acid battery is safe to –26 °C or colder. Storage batteries may be warmed somewhat by charging or discharging. Blow touches or other flame should never be used to heat any type of battery.

A practical discharge limit occurs when the load will no longer operate satisfactorily on the lower output voltage near the “discharged” point. Much gear intended for “mobile” use may be designed for an average of 13.6 V and a peak of perhaps 15 V, but will not operate well below 12 V. For full use of battery charge, the gear should operate well (if not at full power) on as little as 10.5 V with a nominal 12 to 13.6 V rating.

Somewhat the same condition may be seen in the replacement of carbon-zinc cells by NiCd storage cells. Eight carbon-zinc cells will give 12 V, while 10 for the same voltage. If a 10-cell battery holder is used, the equipment should be designed for 15 V in case the carbon-zinc units are plugged in.

5.4.2 Primary batteries

One of the most common primary-cell types is the alkaline cell, in which chemical oxidation occurs during discharges. When there is no current, the oxidation essentially stops until current is required. A slight amount of chemical action does continue, however, so stored batteries eventually will degrade to the point where the battery will no longer supply the desired current.

The alkaline battery has a nominal voltage of 1.5 V. Larger cells capable of production more milliampere hours and less voltage drop than smaller cells. Heavy duty and industrial batteries usually have longer shelf life.

Lithium primary batteries have a nominal voltage of about 3 V per cell and by far the best capacity, discharge, shelf life and temperature characteristics. Their disadvantages are high cost and that they cannot be readily replaced by other types in an emergency.

The lithium-thionyl-chloride battery is a primary cell and should not be recharged under any circumstances. The charging process vents hydrogen, and a catastrophic explosion can result. Even accidental charging caused by wiring errors or a short circuit should be avoided.

Silver oxide (1.5 V) and mercury (1.4 V) batteries are used where nearly constant voltage is desired at low currents for long periods. Their primary application is in small equipment.

Primary batteries should not be recharged for two reasons: it may be dangerous because of heat generated within sealed cells, and even in cases where there may be some success, both the charge and life are limited. One type of alkaline battery is rechargeable and is so marked.

5.4.3 Secondary batteries

The most common type of small rechargeable battery is the nickel-cadmium (NiCd), with a nominal voltage of 1.2 V per cell. Carefully used, these are capable of 500 or more charge/discharge cycles. For long life, the NiCd battery should not be fully discharged. Where there is more than one cell in the battery, the most-discharged cell may suffer polarity reversal, resulting in a short circuit or seal rupture. All storage batteries have discharge limits, and NiCd types should not be discharged to less than 1.0 V per cell. Nickel cadmium cells are not limited to "D" size and smaller cells. They also are available in large varieties ranging to mammoth 1 000 Ah units having carrying handles on the sides and top for adding water, similar to lead-acid types. They are used extensively for uninterruptible power supplies.

For high capacity, the most widely used rechargeable battery is the lead-acid type. In automotive service, the battery is usually expected to discharge partially at a very high rate and then to be recharged promptly while the alternator is also carrying the electrical load. The most appropriate battery for extended high-power electronic applications is the so-called "deep-cycle" battery. These batteries may furnish between 1 000 and 1 200 Wh per charge at room temperature. When properly cared for, they may be expected to last more than 200 cycles. They often have lifting handles and screw terminals, as well as the conventional truncated cone automotive terminals. They may also be fitted with accessories, such as plastic carrying cases, with or without built-in chargers. Lead-acid batteries are also available with gelled electrolyte. Commonly called "gel cells", these may be mounted in any position sensitive.

An automotive lead-acid battery was designed for one task: to deliver a lot of current for a brief period of time. Its output voltage does not remain constant during its discharge cycle, and it is not a good idea to discharge it completely. An automobile battery will not tolerate too many deep-discharge cycles before it's ruined.

A deep-discharge lead-acid battery is much better suited emergency power needs. It can be discharged repeatedly without damage, and will maintain full output voltage over much of its discharge cycle. This type of battery is available at automobile- and marine-parts supply outlets. They are not much more expensive than regular automobile batteries and are designed to deliver moderate current for long periods of time.

The nickel metal hydride (NiMH) battery is similar to the NiCd, but the cadmium electrode is replaced by one made from a porous metal alloy that traps hydrogen; therefore the name of metal hydride. Many of the basic characteristics of these cells are similar to NiCds. For example, the voltage is very nearly the same, they can be slow-charged from a constant current source and they can safety be deep cycled. These are also some important differences: They have higher capacity for the same cell size often nearly twice as much as the NiCd types. The typical size AA NiMH cell has a capacity between 1 000 and 1 300 mAh, compared to the 600 to 830 mAh for the same size NiCd. Another advantage of these cells is a complete freedom from memory effect. NiMH cells do not contain any dangerous substance, while both NiCd and lead-acid cells do contain quantities of toxic heavy metals.

The Lithium-ion (Li-ion) cells is another possible alternative to the NiCd cell. For the same energy storage, it has about one third the weight and one half the volume of NiCd. It also has a lower self-discharge rate. Typically, at room temperature, a NiCd cell will lose from 0.5 to 2% of its charge per day. The lithium-ion cell will lose less than 0.5% per day and even this loss rate decreased after about 10% of the charge has been lost. At higher temperature the difference is even greater. The results are that Lithium-ion cells are a better choice for standby operation where frequent recharge is not available.

One major difference between NiCd and Li-ion cells is the cell voltage. The nominal voltage for NiCd cell is about 1.2 V. For the Li-ion cell it is 3.6 V with a maximum cell charging voltage of 4 V. Li-ion cells cannot be substituted directly for NiCd cells. Chargers intended for NiCd batteries must not be used with Li-ion batteries, and vice versa.

5.5 Inverters

One source of ac power for use in the field is a dc-to-ac converter, or more commonly, an inverter. The ac output of an inverter is a usually square wave. Therefore, some types of equipment cannot be operated from the inverter. Certain types of motor are among those devices that require a sine-wave output. Aside from having a square-wave output, inverters have some other traits that make them less than desirable for field use. Commonly available models do not provide a high power handling capability. Higher power models are available but are quite expensive.

5.6 Generators

For long-term emergency operation, a generator is a requirement. The generator will provide power as long as fuel is available. Proper care is necessary to keep the generator operating reliably, however.

For these periods when the generator is shut down, battery power can be used until the generator can be reactivated. The lubricating oil level should be checked periodically.

If the oil sump becomes empty, the engine can seize, putting the station out of operation and necessitating costly engine repairs.

Remember the engine will produce carbon monoxide gas while it is running. The generator should never run indoors and should be placed away from open windows and doors to keep exhaust fumes from coming inside.

Generators in the 3-5 kW range are easily handled by two people and can provide power for radios and other electrical equipment. Most generators provide 12 V dc output in addition to 120/240 V ac.

Some generators have a continuous power rating and an intermittent power rating. If the total station requirement exceeds the available generator power, transceivers draw full power only while transmitting and that they are not going to be transmitting 100% of the time. It is necessary to ensure that the total possible power consumption does not exceed the intermittent power rating of the generator.

Generators should be tested regularly. Fuel should be fresh. Operator level maintenance (tune-up or oil change) should be performed regularly. Spark plugs should be checked carefully and spare spark plugs should be maintained. The air cleaners should be checked and cleaned according to manufacturer’s instructions.

The generator should be checked for proper operation. If there are any fuel leaks, it should be turned off immediately and the problem corrected. The muffler should be inspected. All protective covers should be in place. The output voltage should be tested. If the generator does not have a built-in over-voltage protector, the voltage should be correct before applying power to radio equipment.

Finally, the generator should be checked for radio noise. Some generators are not fully suppressed for ignition noise. If there is a problem, it may be possible to use resistor-type spark plugs or spark-plug wires. A good Earth ground with a ground rod may help minimize noise.

5.6.1 Installation considerations

Any internal combustion engine is noisy and bothersome when communication equipment is being operated nearby. The placement of a power plant is important, regardless of its size. An engine running at 3 600 rotations per minute, even with an efficient muffler system produces noise and vibration. The engine vibrations are conducted thought the base upon which the engine is mounted to the ground or walls of the building housing the system. Brick or concrete-block construction will reduce the noise level, but if the generator shack is metal, there is less noise abatement. Metal panels may vibrate in sympathy with the sound source add to the din. Applying a hardening caulking compound to the vertical edges of the metal panels cab eliminate some of the noise, as can the use of sound-deadening material in lining the shack.

The distance between the alternator and the operating must be considered. Sound intensity varies inversely with the square of the distance from the source. The noise at a distance of 20 metres will be one-fourth that at a distance of 10 metres. At 30 metres, it will be one ninth.

Fuel consumption must be considered, both from an installation aspect and as a safety problem. Fuel will be used at the rate of 2 to 4 litres per hour is a 2.5-5 kW generator. There should be an ample reserve plan of at least 48 hours of operation. If the fuel is gasoline, safe storage can be a problem. Store gasoline in an area separate from the area housing the generator. Transfer only enough fuel at one time to fill the power unit’s tank. If you in an area where propane or natural gas are available, it might be worthwhile to consider these options as a fuel source. Some alternators are supplied with multiple-fuel capabilities (gasoline or natural gas/propane). A special carburetion system is required for natural gas or propane.

5.6.2 Generator maintenance

Proper maintenance is necessary to obtain rated output and long service life from a gasoline generator. A number of simple measures will prolong the life of the equipment and help maintain reliability.

The manufacturer’s manual should be the primary source of maintenance information and the final word on operating procedures and safety. The manual should be thoroughly covered by all persons who will operate and maintain the unit.

Fuel should be clean, fresh and of good quality. Many problems with gasoline generators are caused by fuel problems. Examples include dirt or water in the fuel land old, state fuel. Gasoline stored for any length of time changes as the more volatile components evaporate. This leaves excess amount of varnish-like substances that will clog carburettor passages. If the generator will be stored for a long period, it is good to run it until all of the fuel is burned. Faulty spark plugs are a common cause of ignition problems. Spare spark plugs should be kept with the unit, along with tools needed to charge them.

5.6.3 Generator earth ground

A proper ground for the generator is necessary for both safety reasons and to ensure proper operation of equipment powered from the unit. Most generators are supplied with a three-wire outlet. Some generators require that the frame be grounded also. An adequate pipe or rod should be driven into the ground near the generator and connected to the provided clamp or lug.

5.7 Solar power

A solar cell is a very simple semiconductor. Solar cells are, in fact, large-area semiconductor diodes. Simply explained, when the photons contained in light rays bombard the barrier of this semiconductor, hole electron pairs inside this P-N junction are freed, resulting in a forward bias of the junction, just as in phototransistors. This forward-biased junction can deliver current into a load. Because the exposed area of a solar cell can be quite large, the forward current proceed can be substantial. It follows that the output current of a photocell is directly proportional to the rate of photon bombardment, and thus to the exposed are of the photocell.

5.7.1 Types of solar cells

Originally, solar cells were made by cutting slides of grown silicon-crystal rod and subjecting them to doping and metallization process. These solar cells are called monocrystalline cells because each unit consists of only one crystal plate. The shape of these cells is the same as that of the silicon rod from which they are cut: round. A slice of this material with an area of 50 mm can be made into one photocell, but a slice of this size could also be used to produce upwards of a thousands transistors.

Most are polarity protected with a diode in series with the positive voltage line. When it gets dark, and the output voltage drops, the diode ensures that the panel won't start drawing current from the battery.

Solar panels typically deliver 15 to 18 V at 600 to 1 500 mA in full sunlight. This will not damage a high-capacity battery, such as a deep-cycle unit. All you need do is hook up the battery, put the solar panel in full sunlight, and charge away. The battery will regulate the maximum voltage from the panel.

If you're going to use a solar panel to recharge a smaller battery, such as a Nickel-Cadmium (NiCd) battery or gelled-electrolyte lead-acid battery, you'll need to pay a bit more attention to detail. These types of batteries can suffer damage if charged too quickly, so a regulated charge is necessary.

A dc-ac converter, or inverter converts 12 V to a square-wave ac output at approximately 60 Hz. Inverters are limited to about 100 to 400 watts, however, and some equipment (especially motors) cannot be powered by a square wave. An inverter will run a few light bulbs or a small soldering iron and can be a useful addition to a battery-operated station. Some newer ones use switching technology and are quite lightweight.

Polycrystalline cells are typically manufactures as rectangular blocks of seemingly randomly arranged silicon crystals from which the cell plates are cut. These cells are recognized by their shape, random pattern and colourful surface. Polycrystalline cells are less expensive to manufacture than monocrystalline cells. Reliable amorphous panels are available from many manufactures. These panels come in several forms: mounted on thin glass, framed, and even mounted on flexible substrates, such as steel.

5.7.2 Solar cell specifications

Depending on construction, each cell has an open-circuit, when exposed to the sun, of 0.6 to 0.8 V. This output voltage drops somewhat when current is drawn from a solar cell. This is called the cell's *load curve*. Open-circuit voltage is approximately 0.7, and output voltage at optimum load is normally 0.45. Output current is maximum with shorted output terminals. This maximum current is called the short-circuit current, and is dependent on the cell type and size. Because a cell's output current remains relatively constant under varying load conditions, it can be considered to be a constant-current sources.

As with batteries, solar cells may be operated in series to increase output voltage, and/or in parallel to increase output-current capability. Several manufactures supply arrays or panels with a number of cells in a series-parallel hook-up to be used, for example, for battery charging.

Techniques have been developed for the construction of amorphous cells whereby the cells are manufactured in series by cutting metal layers that have been vapour deposited on the amorphous silicon mass. This cutting is done with a laser. Cell width is such panels may be up to several feet, and the output-current capability of these relatively economical panels is excellent.

Solar-cell efficiency varies: Monocrystalline cell have efficiencies up to 15%; polycrystalline cells, 10 to 12%; amorphous cells, 6.5 to over 10%, depending on the manufactures process.

The output power of solar arrays or panels is specified in watts. Typically, the listed wattage is measured at full exposure to sunlight, at a nominal potential of 7 V for a 6-V system, 14 V for a 12-V system, and so on. You can calculate the maximum current that can be expected from a solar panel by dividing the specified output power by the panel voltage.

5.7.3 Storing solar energy

Because the sun does not shine 24 hours per day at many locations, some means of storing collected energy must be used. Batteries are commonly used for this purpose. Battery capacity is generally expressed in ampere-hours (Ah) or milliampere-hours (mAh). This rating is simply the product of discharge current and discharge time in hours. For example, a fully charge 500-mAh NiCd battery of good quality can deliver a discharge current of 100 mA for a period of 5 hours, or 200 mA for 2½ hours before recharging is required. Three types of rechargeable batteries are commonly used:

Nickel-cadmium (NiCd) batteries: NiCd are mostly used in relatively low energy applications such as hand-held transceivers, scanners, etc. The development of consumer electronics has contributed to the rapidly increasing availability (and somewhat-less-rapidly decreasing cost) of NiCd. Major advantage of NiCd: They are hermetically sealed, operate in any position and have a good service life (several hundred charge/discharge cycles), if they are properly maintained.

Gelled-electrolyte lead-acid batteries: These hermetically sealed batteries are available in capacities from below 1 Ah to more than 50 Ah. They are ideal for supplying energy to a radio station, but their cost (for capacities above 10 Ah) is rather high. For portable and low power stations, thought, this type of battery is difficult to beat. The cells can be operated in any position, but should be charged in an upright position. If properly maintained (no deep discharges-cell polarity reversal is possible under these conditions-and they stored in a fully charged state), gel cells last a long time (500 or so cycles).

Other lead-acid batteries: These are available in the standard automotive version, in the marine/ recreational vehicle deep-discharge version and in the golf-cart variety. Differences: Automotive batteries usually fail (because of the thin plate and insulation material used in their construction), resulting in premature internal short circuits. Golf-cart and marine/recreational vehicle batteries have thicket plated with more rigid insulation between them, so these batteries can with stand deeper discharge without plate deformation and internal failure. Deep discharge batteries provide the best value in a ham station. Some of these batteries require attention (the electrolyte level must be maintained), and they last longest when kept charged. Because these batteries use a wet electrolyte (water), and most of them are not hermetically sealed, they must be kept upright.

5.7.4 A typical application

Here's a practical example of how to calculate power requirements for a solar-powered HF radio station. The first thing to do is define the power demand. Assume a 100-W transmitter. The assumption is that 100 W is the peak power consumption, and occurs only during CW operation and SSB voice peaks when a 13.6-V nominal supply (a fully charged battery) is provided.

The most reliable way to calculate realistic power requirements is to determine the power used over a longer period of time (say) a week or month. Because most of us have more or less recurring weekly habits, we'll take one week as the base period. (One can substitute numbers to adapt this calculation for the transmitter, under typical operating circumstances.) Assume that the transmitter is turned on five days. Of each two-hour period, 1½ hours is spent listening, and transmitting takes the remaining half hour. Assume that the current consumption of the transceiver during receive is 2 A; during the 100-W peaks on transmit, current drawn is 20 A. The owner's manual for transmitter should give the maximum dc current drain. The average current consumption during SSB transmitting is only about 4 A. Therefore, we need a battery that can supply a peak current of at least 20 A and an average current of 4 A. Now calculate the total energy consumed in ampere hours over a one-week period:

Receiving: 2 A × 2½ hours/day × 5 days = 25 Ah

Transmitting: 4 A × ½ hours/day × 5 days = 10 Ah

The total energy used per week is 25 + 10 = 35 Ah, or per day (average) is 35 ÷ 7 = 5 Ah. If we had a perfect system, all we would need to do is supply 35 Ah per week (5 Ah per day) to the battery. In practice, imperfections in battery construction cause some loss (self discharge), for which the charging system must compensate.

Next, calculate the minimum battery capacity required for this application. The system should be designed so that sufficient energy is available to run the equipment for two consecutive sunless days (this is rather arbitrary – some locations are worse than others in this regard). Because these sun less days could be days on which operation is necessary and because it is not good to discharge a battery to less than 50% of its capacity (for maximum battery life), this battery must have a capacity of lest 2 (days) × 5 Ah) ÷ 0.5 (for the 50% charge capacity left after 3 days without sunshine) = 20 Ah. If the location is likely to be without sunshine for as much as an entire week, the battery requirement would be 7 ´ 5 ÷ 0.5 = 70 Ah. Add about 10% to this number to compensate for self-discharge and other losses. (Typically, this means to procure the next-larger-size battery than the initial calculations indicated.)

To keep the battery sufficiently charged, firstly estimate the average number of hours of sunshine per year in the area. This information can be found in an almanac. As a guide, average annual sun exposure is approximately 3 200 hours per year in sunny regions, less elsewhere (down to about 1 920 hours per year in the far northern climates).

The solar panel should be mounted in a fixed position with an optimum angle relative to the Earth. In temperate zones, it could vary from about 30° in the summer up to about 60° in winter. Fixed-mounted solar panels cannot pick up maximum energy from the sun, for obvious reasons. In practice, they receive only 70% of the total sunlit time, which is anywhere between 1 340 and 2 240 hours per year (between 26 and 43 hours per week), depending on location.

The remaining system planning is easy. Earlier calculations showed that the solar cells must replenish 35 Ah per week, plus 10% to compensate for losses, or about 38.5 Ah or battery capacity. With solar energy available in the Sunbelt for 43 hours per week, the required charge current is 38.5 Ah ÷ 43 hours of sunshine = 0.9 A. In the northern part of the US, this is 38.5 Ah ÷ 25.8 hours = 1.5 A.

In the 12-V system described here, the solar panel operates, with a fully charged battery at about 13.6 V, plus the voltage drop of a series diode. With a fully loaded panel voltage of 14 V, a panel rated at 21 W (14 V × 1.5 A) is required in northern climes. In practice, this power can be obtain from good quality solar panel with a surface area as small as 65 cm^2. In sunny regions only 12.6 W (14 V × 0.9 A) of solar energy may be needed.

5.7.5 Some practical hints

Solar panels can be wired in series to provide increased output voltage. If the total output of the cell array exceeds 20 V, shunt diodes may be wired across each solar cells. Similarly, solar panels can be wired in parallel to yield increased output-current capability.

A series diode should be installed to prevent discharge of the battery into the panels. A Schottky diode can be used in applications where it is important to maintain the lowest voltage drop (and minimum loss of charge current).

Precaution should be taken to prevent battery overcharging and related gas discharge inside the battery. Several manufacturers supply simple charge regulators that serve this purpose by disconnecting the solar panel from the battery when the battery is fully charged. Some of these chargers allow charging to resume when the battery has reached a measurable level of discharge.

Note: These values are only valid for lead-acid batteries; and entirely different set of charge criteria exists for NiCds.

5.7.6 Installing solar panels

If you plan to permanently install solar panels, consider mounting them at ground level on a simple wooden or metal frame, or mounting the m on the roof. Roof mounting is more appropriate if you have a roof that slopes at the correct angle (30-60°), and in the right direction (anywhere between a kittle east of south and southwest is acceptable). The easiest way to mount panels permanently is with a silicone adhesive. First, series diodes should be mounted on the back of each panel.

If the solar panels are going to be located in an area where they might be subjected to lightning, it is especially important to ground the metal frames of the solar panels. A separate wire should be used for this earth ground, that is, not combined with one of the power leads.

6 Repeaters and trunked networks

6.1 Communication beyond line-of-sight through relays

At VHF and UHF, some type of relay system or network is required for reliable communications beyond line-of-sight.

6.2 Terrestrial repeater

A single repeater station in a favourable location (on a hill or atop a building) may be used to retransmit signals between points not having line-of-sight.

6.3 Trunked land mobile radio systems with a central controller

Trunking is the automatic sharing of a common pool of possibly 10 or more frequencies in a multiple repeater system. Trunking may be performed at a single site or multiple sites for wide-area coverage.

Trunked systems are based on the premise that each user transmits only a small percentage of time, thus it is possible to provide more overall capacity with a band than if each station or group of users had its own frequency. Linked repeaters provide better geographical coverage than a single repeater. A trunked network includes some redundancy, which can be beneficial in disaster situations. If prearranged, trunked systems may include an emergency feature for speech or data calls to specified mobile units.

A trunked system has at least one control channel that continuously transmits the computer-generated digital data needed to control vehicular and hand-held radios within range. Channels are assigned to a group only when there is traffic, making the channels free for other users. This is accomplished in a way that users hear only the traffic intended for their group and in a way that is completely transparent to the users. There are two types of trunking control systems, known as dedicated control channel and distributed control channel. In the dedicated control system, the control channel operates on one frequency. The distributed type uses any idle channel for control transmissions.

Mobile units are assigned identifiers and a home repeater. When a mobile unit is not transmitting, it always monitors the home repeater for data messages. When a mobile transmits, it identifies through a digital handshake protocol that takes only a fraction of a second.

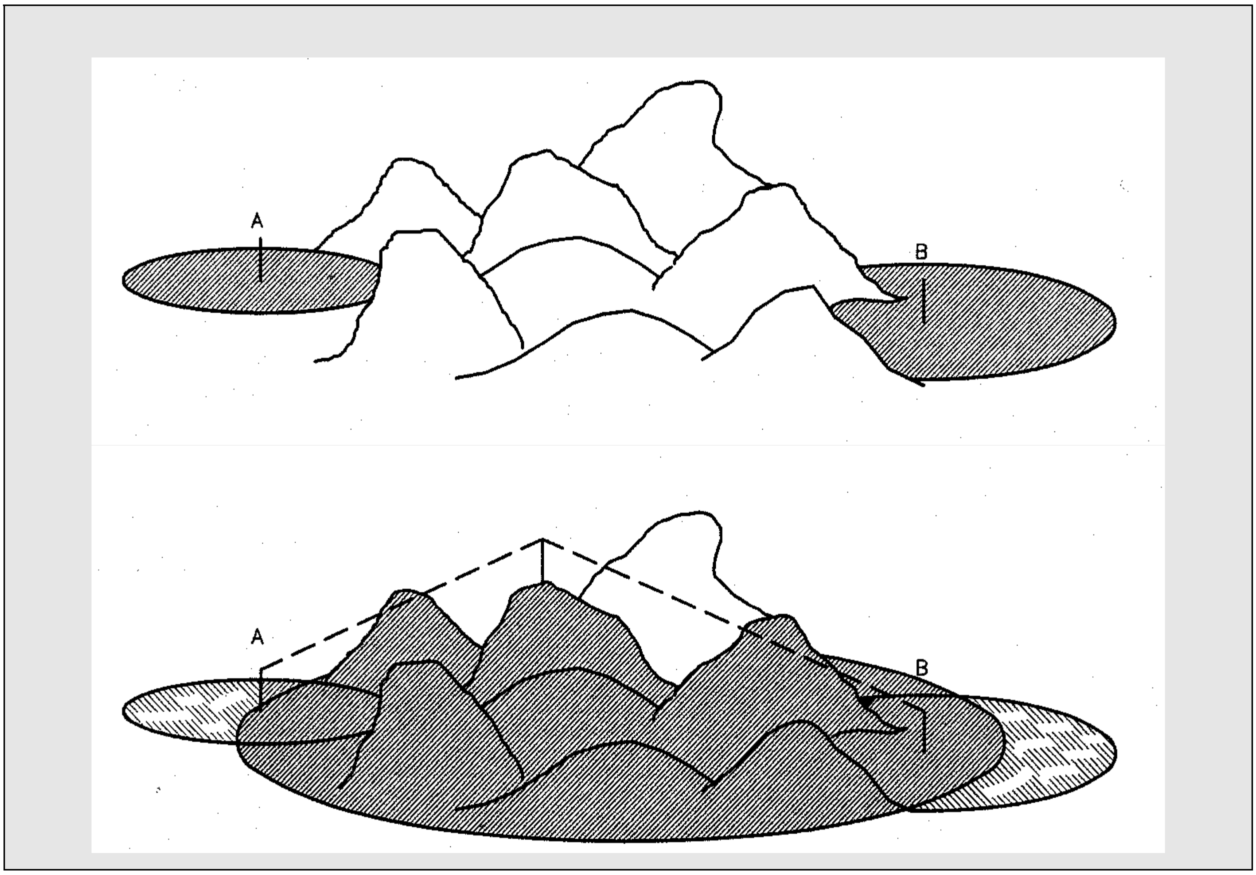
Characteristics of digital land mobile systems are described in Report ITU-R M.2014. These systems include a trunked and non-trunked capability to permit direct mobile-to-mobile and group speech call facilities with user options to permit selective and secure calling.

6.4 Trunked land mobile radio systems without a central controller

There are also trunking systems using multi-channel access techniques and appropriate protocols that do not require a central controller for the detection of an idle radio channel, known as “Personal Radio System” and “Digital Short Range Radio”. Both systems work in the 900 MHz frequency band. They provide up to 80 channels and use a transmit power of up to 5 W. More detailed data of these systems are given in Recommendation ITU-R M.1032.

Figure 16 – Repeater stations

In the top drawing, stations A and B are unable to interoperate because propagation is blocked by hills. In the bottom drawing, a repeater station is able to relay signals between stations A and B.



All radios in these systems are normally in the standby state on a control channel, ready to receive a selective calling signal. A calling station looks for and finds an idle traffic channel and stores its number in its memory. Then the calling station transmits on a control channel, a selective calling signal including at least its own identity, the identity of the called station and the number of the identified idle channel. The standby stations detecting their identity code in the received signal, move to the indicated traffic channel and enter into communication. At the end of the communication all units return again to the standby mode.

List of commonly used abbreviations

A	Ampere
ac	Alternating current
A/D	Analogue-to-digital
Ah	Ampere-hour
AM	Amplitude Modulation
AMTOR	Amateur Teleprinting Over Radio
ARES	Amateur Radio Emergency Service
ARQ	Automatic Repeat reQuest (error-control technique)
AX.25	Amateur Packet Radio Link Layer Protocol
CANTO	Caribbean Association of National Telecommunications Operators
CDERA	Caribbean Disaster Emergency Response Agency
CENTREX	Central Exchange
CEO	Chief Executive Officer
COW	Cell On Wheels
CP	Command Post
CQ	General Call (to all radio stations)
CW	Carrier Wave (Morse radiotelegraphy)
DAMA	Demand Assigned Multiple Access
DECT	Digital Enhanced Cordless Telephone
DDI	Direct Dial In
DHA	Department of Humanitarian Affairs (now OCHA)
DMT	Disaster Management Team (UN)
DSC	Digital Selective Calling
DSL	Digital Subscriber Line
DSP	Digital Signal Processing
EDGE	Enhanced Data Rates for GSM Evolution
ELT	Emergency Location Transmitter
EOC	Emergency Operations Centre
Fax	Facsimile
FD	Field Day (amateur)
FEC	Forward Error Control
FM	Frequency Modulation
FSTV	Fast Scan Television

FTP	File Transfer Protocol
GAN	Global Area Network
GETS	Government Emergency Telecommunications
GLONASS	Global Navigation Satellite System
GMDSS	Global Maritime Distress and Safety System
GMPCS	Global Mobile Personal Communications by Satellite
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSO	Geostationary Orbit (satellite)
GTC	Grameen Telecom
HAZMAT	Hazardous Materials
HF	High Frequencies (3-30 MHz)
HTML	Hypertext Markup Language
IAPSO	The Inter-Agency Procurement Services Office (UNDP)
IARU	International Amateur Radio Union (NGO)
IASC	Inter Agency Standing Committee (UN advisory body)
ICAO	International Civil Aeronautical Organisation
ICET	Intergovernmental Conference on Emergency Telecommunications
ICRC	International Committee of the Red Cross
IDNDR	International Decade for Natural Disaster Reduction
IEPREP	Internet Emergency Preparedness
IF	Intermediate Frequency
IFRC	International Federation of Red Cross and Red Crescent Societies
IMO	International Maritime Organization
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITA	International Telegraph Alphabet
ITU	International Telecommunication Union
ITU-D	Telecommunication Development Sector (ITU)
ITU-R	Radiocommunication Sector (ITU)
ITU-T	Telecommunication Standardization Sector (ITU)
kW	Kilowatt
LAN	Local Area Network
LEO	Low Earth Orbit (satellite)
LES	Land Earth Station

MESA	Mobility for Emergency and Safety Applications
MMSI	Maritime Mobile Service Indicator
NCS	Net Control Station
NGN	Next-Generation Networks
NGO	Non-governmental organization
NiCd	Nickel Cadmium (cell)
NiMH	Nickel Metal Hydride (cell)
NOTAM	Notice to Airmen
NVIS	Near-vertical-incidence-sky wave (propagation)
OCHA	Office for the Coordination of Humanitarian Affairs (UN)
OSOCC	On-side Operations Coordination Centre
PACSAT	Packet (radio) Satellite
PACTOR	Packet Transmission Over Radio
PBBS	Packet Bulletin Board System
PBX	Private Branch Exchange
PCS	Personal Communications Systems
PLB	Personal Locator Beacon
PLMN	Public Land Mobile Network
POP	Post Office Protocol
POTS	Plain Old Telephone System
PSAP	Public Access Point
PSTN	Public Switched Telephone Network
RBGAN	Regional Broadband Global Area Network
RBS	Radio base station
RF	Radio frequency
ROBO	Remote Office – Branch Office
RTTY	Radioteletype (narrow band direct-printing radiotelegraph)
SCIP	Secure Communication Interoperability Protocol
SDR	Swiss Disaster Relief
SELCAL	Selective Calling
SET	Simulated Emergency Test
SITOR	Simplex Teletype Over Radio (narrow band direct-printing radiotelegraphy system used in the maritime mobile service)
SOHO	Small Office – Home Office
SOLAS	Safety of Life at Sea

SRSA	Swedish Rescue Services Agency
SSB	Single Sideband
SSTV	Slow Scan Television
SWR	Standing Wave Ratio
TCP/IP	Transmission Control Protocol/Internet Protocol
TCO	Telecommunications Coordination Officer
TNC	Terminal Node Controller (packet radio)
UNHCR	United Nations High Commissioner for Refugees
UNDAC	United Nations Disaster Assessment and Coordination
UNDP	United Nations Development Programme
UNICEF	United Nations Children’s Fund
UNOG	United Nations Organisation Geneva
UHF	Ultra High Frequencies (30-3 000 MHz)
USAT	Ultra Small Aperture Terminal
USB	Upper Side Band
USD	United States Dollar
UWB	Ultra WideBand
V	Volt
VHF	Very High Frequencies (30-300 MHz)
VPN	Virtual Private Network
VITA	Volunteers in Technical Assistance
VSAT	Very Small Aperture Terminal
W	Watt
WAN	Wide Area Network
WAP	Wireless Access Protocol
WFP	World Food Programme
WHO	World Health Organization (UN)
Wi-Fi	Wireless Fidelity
WLL	Wireless Local Loop (generally replaced by fixed wireless access (FWA)
WTDC	World Telecommunication Development Conference
WGET	Working Group on Emergency Telecommunications
WRC	World Radiocommunication Conference
WWRF	World Wide Research Forum
WWW	World Wide Web

Morse code signals[2]

1.1 The following are the written characters that may be used and the corresponding Morse code signals:

1.1.1 *Letters*

	a .-	i ..	r .-.
	b -…	j .---	s …
	c -.-.	k -.-	t -
	d -..	l .-..	u ..-
	e .	m --	v …-
accented	e ..-..	n -.	w .--
	f ..-.	o ---	x -..-
	g --.	p .--.	y -.--
	h ….	q --.-	z --..

1.1.2 *Figures*

1 .----	6 -….
2 ..---	7 --…
3 …--	8 ---..
4 …-	9 ----.
5 …..	0 -----

1.1.3 *Punctuation marks and miscellaneous signs*

Full stop (period)	[.]	.-.-.-
Comma	[,]	--..--
Colon or division sign	[:]	---…
Question mark (note of interrogation or request for repetition of a transmission not understood)	[?]	..--..
Apostrophe	[’]	.----.
Hyphen or dash or subtraction sign	[-]	-….-
Fraction bar or division sign	[/]	-..-.
Left-hand bracket (parenthesis)	[(]	-.--.
Right-hand bracket (parenthesis)	[)]	-.--.-
Inverted commas (quotation marks)(before and after the words)	[“”]	.-..-.
Double hyphen	[=]	-…-
Understood		…-.
Error (eight dots)		……..
Email (at) Sign	[@]	---.--.
Cross or addition sign	[+]	.-.-.
Invitation to transmit		-.-
Wait		.-…
End of work		…-.-
Starting signal (to precede every transmission)		-.-.--
Multiplication sign	[x]	-..-

2 From Recommendation ITU-T F.1 Division B.

Phonetic alphabet code[3]

Letter to be transmitted	Code word to be used	Spoken as
A	Alfa	AL FAH
B	Bravo	BRAH VOH
C	Charlie	CHAR LEE or SHAR LEE
D	Delta	DELL TAH
E	Echo	ECK OH
F	Foxtrot	FOKS TROT
G	Golf	GOLF
H	Hotel	HOH TELL
I	India	IN DEE AH
J	Juliett	JEW LEE ETT
K	Kilo	KEY LOH
L	Lima	LEE MAH
M	Mike	MIKE
N	November	NO VEM BER
O	Oscar	OSS CAH
P	Papa	PAH PAH
Q	Quebec	KEH BECK
R	Romeo	ROW ME OH
S	Sierra	SEE AIR RAH
T	Tango	TANG GO
U	Uniform	YOU NEE FORM or OO NEE FORM
V	Victor	VIK TAH
W	Whiskey	WISS KEY
X	X-ray	ECKS RAY
Y	Yankee	YANG KEY
Z	Zulu	ZOO LOO

3 From Radio Regulations Appendix S14.

Figure code[4]

Figure or mark to be transmitted	Spoken as (ICAO)	Code word (Appendix S14)	Spoken as (Appendix S14)
0	ZE-RO	Nadazero	NAH-DAH-ZAY-ROH
1	WUN	Unaone	OO-NAH-WUN
2	TOO	Bissotwo	BEES-SOH-TOO
3	TREE	Terrathree	TAY-RAH-TREE
4	FOW er	Kartefour	KAR-TAY-FOWER
5	FIFE	Pantafive	PAN-TAH-FIVE
6	SIX	Soxisix	SOK-SEE-SIX
7	SEV en	Setteseven	SAY-TAY-SEVEN
8	AIT	Oktoeight	OK-TOH-AIT
9	NIN er	Novenine	NO-VAY-NINER
Decimal point	DAY SEE MAL	Decimal	DAY-SEE-MAL
Hundred	HUN dred		
Thousand	TOU SAND		

4 From ICAO Radiotelephony Procedures.

Q Code[5]

Certain Q code abbreviations may be given an affirmative or negative sense by sending, immediately following the abbreviation, the letter C or the letters NO (in radiotelephony spoken as: CHARLIE or NO).

The meanings assigned to Q code abbreviations may be amplified or completed by the addition of other appropriate groups, call signs, place names, figures, numbers, etc. It is optional to fill in the blanks shown in parentheses. Any data which are filled in where blanks appear shall be sent in the same order as shown in the text of the following tables.

Q code abbreviations are given the form of a question when followed by a question mark in radiotelegraphy and RQ (ROMEO QUEBEC) in radiotelephony. When an abbreviation is used as a question and is followed by additional or complementary information, the question mark (or RQ) should follow this information.

All times shall be given in Coordinated Universal Time (UTC) unless otherwise indicated in the question or reply.

Abbreviation	Question	Answer or Advice
QRA	What is the name of your vessel (*or* station)?	The name of my vessel (*or* station) is …
QRB	How far approximately are you from my station?	The approximate distance between our stations is … nautical miles (*or* kilometres).
QRG	Will you tell me my exact frequency (*or* that of …)?	Your exact frequency (*or* that of …) is ... kHz (*or* MHz).
QRH	Does my frequency vary?	Your frequency varies.
QRI	How is the tone of my transmission?	The tone of your transmission is … 1. good 2. variable 3. bad.
QRK	What is the intelligibility of my signals (*or* those of … *(name and/or call sign)*)?	The intelligibility of your signals (*or* those of … *(name and/or call sign)*) is … 1. bad 2. poor 3. fair 4. good 5. excellent.
QRL	Are you busy?	I am busy (*or* I am busy with … *(name and/or call sign)*). Please do not interfere.

5 From Recommendation ITU-R M.1172, *Miscellaneous abbreviations and signals to be used for radiocommunications in the maritime mobile service*, Radio Regulations (1998).

Abbreviation	Question	Answer or Advice
QRM	Is my transmission being interfered with?	Your transmission is being interfered with … 1. nil 2. slightly 3. moderately 4. severely 5. extremely.
QRZ	Who is calling me?	You are being called by … (on … kHz (*or* MHz)).
QSA	What is the strength of my signals (*or* those of … *(name and/or call sign)*)?	The strength of your signals (*or* those of … *(name and/or call sign)*) is … 1. scarcely perceptible 2. weak 3. fairly good 4. good 5. very good.
QSB	Are my signals fading?	Your signals are fading.
QSO	Can you communicate with … *(name and/or call sign)* direct (*or* by relay)?	I can communicate with … *(name and/or call sign)* direct (*or* by relay through …).
QSP	Will you relay to … *(name and/or call sign)* free of charge?	I will relay to … *(name of and/or call sign)* free of charge.
QSV	Shall I send a series of Vs (*or* signs) for adjustment on this frequency (*or* on … kHz (or MHz))?	Send a series of Vs (*or* signs) for adjustment on this frequency (*or* on … kHz (or MHz)).
QSW	Will you send on this frequency (*or* on … kHz (*or* MHz)) (with emissions of class …)?	I am going to send on this frequency (*or* on … kHz (*or* MHz)) (with emissions of class …).
QSX	Will you listen to … *(name and/or call sign(s))* on … kHz (*or* MHz), or in the bands …/ channels …?	I am listening to … *(name and/or call sign(s))* on … kHz (*or* MHz), or in the bands …/channels …
QSY	Shall I change to transmission on another frequency?	Change to transmission on another frequency (*or* on … kHz (*or* MHz)).
QSZ	Shall I send each word or group more than once?	Send each word or group twice (*or* … times).
QTA	Shall I cancel telegram (*or* message) number …?	Cancel telegram (*or* message) number …
QTC	How many telegrams have you to send?	I have … telegrams for you (*or* for … (*name and/or call signs*)).
QTH	What is your position in latitude and longitude *(or according to any other indication)*?	My position is … latitude, … longitude *(or according to any other indication).*
QTR	What is the correct time?	The correct time is … hours.

Miscellaneous abbreviations and signals[6]

Abbreviation or signal	Definition
AA	All after … *(used after a question mark in radiotelegraphy or after RQ in radiotelephony (in case of language difficulties) or after RPT, to request a repetition).*
AB	All before … *(used after a question mark in radiotelegraphy or after RQ in radiotelephony (in case of language difficulties) or after RPT, to request a repetition).*
ADS	Address *(used after a question mark in radiotelegraphy or after RQ in radiotelephony (in case of language difficulties) or after RPT, to request a repetition).*
$\overline{\text{A}}$	End of transmission.
$\overline{\text{AS}}$	Waiting period.
BK	Signal used to interrupt a transmission in progress.
BN	All between … and … *(used after a question mark in radiotelegraphy or after RQ in radiotelephony (in case of language difficulties) or after RPT, to request a repetition).*
BQ	A reply to an RQ.
$\overline{\text{BT}}$.	Signal to mark the separation between different parts of the same transmission.
C	Yes *or* "The significance of the previous group should be read in the affirmative".
CFM	Confirm (*or* I confirm).
CL	I am closing my station.
COL	Collate (*or* I collate).
CORRECTION	Cancel my last word *or* group. The correct word *or* group follows *(used in radiotelephony, spoken as KOR-REK-SHUN).*
CQ	General call to all stations.
CS	Call sign *(used to request a call sign).*
DE	"From …" *(used to precede the name or other identification of the calling station).*
K	Invitation to transmit.
$\overline{\text{KA}}$	Starting signal.
MIN	Minute (*or* Minutes).
NIL	I have nothing to send to you.
NO	No *(negative).*
NW	Now.
OK	We agree (*or* It is correct).
PBL	Preamble *(used after a question mark in radiotelegraphy or after RQ in radiotelephony (in case of language difficulties) or after RPT, to request a repetition).*

6 From Recommendation ITU-R M.1172, *Miscellaneous abbreviations and signals to be used for radiocommunications in the maritime mobile service*, Radio Regulations (1998).

Abbreviation or signal	**Definition**
PSE	Please.
R	Received.
REF	Reference to … (*or* Refer to …).
RPT	Repeat (*or* I repeat) (*or* Repeat …).
RQ	Indication of a request.
SIG	Signature *(used after a question mark in radiotelegraphy or after RQ in radiotelephony (in case of language difficulties) or after RPT, to request a repetition).*
SVC	Prefix indicating a service telegram.
SYS	Refer to your service telegram.
TFC	Traffic.
TU	Thank you.
TXT	Text *(used after a question mark in radiotelegraphy or after RQ in radiotelephony (in case of language difficulties) or after RPT, to request a repetition).*
$\overline{\text{VA}}$	End of work.
WA	Word after … *(used after a question mark in radiotelegraphy or after RQ in radiotelephony (in case of language difficulties) or after RPT, to request a repetition).*
WD	Word(s) *or* Group(s).
WX	Weather report (*or* Weather report follows).

Note: When used in radiotelegraphy, a bar over the letters composing a signal denotes that the letters are to be sent as one signal.

Procedure words[7]

Signal strength and readability

Signal strength	
Spoken	**Meaning**
LOUD	Your signal is strong.
GOOD	Your signal is good.
WEAK	I can hear you but with difficulty.
VERY WEAK	I can hear you but with great difficulty
NOTHING HEARD	I cannot hear you at all.

Readability	
Spoken	**Meaning**
CLEAR	Excellent quality.
READABLE	Good quality, no difficulty in reading you.
DISTORTED	I have problems reading you.
WITH INTERFERENCE	I have problems reading you due to interference.
NOT READABLE	I can hear that you are transmitting but cannot read you at all.

Procedure word	Meaning
ACKNOWLEDGE	Confirm that you have received my message and will comply (WILCO)
AFFIRMATIVE	Yes/Correct
ALL AFTER	Everything that you transmitted after …
ALL BEFORE	Everything that you transmitted before …
BREAK	Indicates separation of text from rest of message.
BREAK BREAK	I wish to interrupt an ongoing exchange of transmissions in order to pass an urgent message.
CALL SIGN	The group that follows is a call sign.
CANCEL	Annul the previously transmitted message.
CORRECT	You are correct or what you have transmitted is correct.
CORRECTION	An error has been made in this transmission (or message indicated). The correct version is …

7 Adapted from UNHCR Procedure for Radio Communication and supplemental sources.

Procedure word	Meaning
DISREGARD	Consider that transmission as not sent.
DO NOT ANSWER – OUT	Station(s) called are not to answer this call, acknowledge this message, or to transmit in connection with this transmission
FIGURES	Numerals or numbers will follow.
HOW DO YOU READ?	What is the readability of my signal?
I SAY AGAIN	I repeat for clarity or emphasis.
MESSAGE FOLLOWS	I have a formal message which should be recorded (e.g.) written down
MONITOR	Listen out on … (frequency).
NEGATIVE	No/Incorrect
OVER	This is the end of this transmission and a response is necessary.
OUT	This is the end of my transmission. No answer is required or expected. (OVER and OUT are never used together.)
READ BACK	Repeat this entire transmission back to me exactly as received.
RELAY (TO)	Transmit the following message to all addressees or to the address immediately following …
REPORT	Pass me the following information …
ROGER	I have received your last transmission. (Not an answer to a question.)
SAY AGAIN	Repeat your last transmission or repeat the portion indicated by “ALL AFTER”.
SILENCE	Cease all transmission immediately. Maintain until lifted.
SILENCE LIFTED	Transmissions may resume after SILENCE has been previously ordered.
SPEAK SLOWER	Your transmissions are too fast. Reduce speed.
UNKNOWN STATION	The identity of the station heard is unknown.
VERIFY	Verify the entire message (or portion indicated) with the originator and send corrected version. To be used only when the addressee has serious questions about the validity of the message.
WAIT	Wait for a few seconds.
WAIT OUT	Wait for a longer period. I will re-establish contact when I return on the air.
WILCO	I have received your message and will comply. (ROGER is implied but not stated.)
WORD AFTER	The word of the message to which I refer is that which follows …
WORD BEFORE	The word of the message to which I refer is that which precedes …
WORDS TWICE	Communication is difficult. Transmit each word or phrase twice.
WRONG	The last transmission was incorrect. The correct version is …

RECOMMENDATION ITU-R P.1144-1

GUIDE TO THE APPLICATION OF THE PROPAGATION METHODS OF RADIOCOMMUNICATION STUDY GROUP 3

(1995-1999)

The ITU Radiocommunication Assembly,

considering

a) that there is a need to assist users of the ITU-R Recommendations P Series (developed by Radiocommunication Study Group 3),

recommends

1 that the information contained in Table 1 be used for guidance on the application of the various propagation methods contained in the ITU-R Recommendations P Series (developed by Radiocommunication Study Group 3).

NOTE 1 – For each of the ITU-R Recommendations in Table 1, there are associated information columns to indicate:

Application: the service(s) or application for which the Recommendation is intended.

Type: the situation to which the Recommendation applies, such as point-to-point, point-to-area, line-of-sight, etc.

Output: the output parameter value produced by the method of the Recommendation, such as path loss.

Frequency: the applicable frequency range of the Recommendation.

Distance: the applicable distance range of the Recommendation.

% *time:* the applicable time percentage values or range of values of the Recommendation; % time is the percentage of time that the predicted signal is exceeded during an average year.

% *location:* the applicable per cent location range of the Recommendation; % location is the percentage of locations within, say, a square with 100 to 200 m sides that the predicted signal is exceeded.

Terminal height: the applicable terminal antenna height range of the Recommendation.

Input data: a list of parameters used by the method of the Recommendation; the list is ordered by the importance of the parameter and, in some instances, default values may be used.

The information, as shown in Table 1, is already provided in the Recommendations themselves; however, the table allows users to quickly scan the capabilities (and limitations) of the Recommendations without the requirement to search through the text.

Table 1 – ITU-R radiowave propagation prediction methods

Method	Application	Type	Output	Frequency	Distance	% time	% location	Terminal height	Input data
Rec. ITU-R P.368	All services	Point-to-point	Field strength	10 kHz to 30 MHz	1 to 10 000 km	Not applicable	Not applicable	Ground-based	Frequency Ground conductivity
Rec. ITU-R P.370	Broadcasting	Point-to-area	Field strength	30 MHz to 1 000 MHz	10 to 1 000 km	1, 5, 10, 50	1 to 99	Tx: effective height from less than 0 m to greater than 1 200 m Rx: 1.5 to 40 m	Distance Tx antenna height Frequency Percentage time Rx antenna height Terrain clearance angle Terrain irregularity Percentage locations
Rec. ITU-R P.1147	Broadcasting	Point-to-area	Sky-wave field strength	0.15 to 1.7 MHz	50 to 12 000 km	10, 50	Not applicable	Not applicable	Latitude and longitude of Tx Latitude and longitude of Rx Distance Sunspot number Tx power Frequency
Rec. ITU-R P.452	Services employing stations on the surface of the Earth; interference	Point-to-point	Path loss	700 MHz to 30 GHz	Not specified but up to and beyond the radio horizon	0.001 to 50 Average year and worst month	Not applicable	No limits specified	Path profile data Frequency Percentage time Tx antenna height Rx antenna height Latitude and longitude of Tx Latitude and longitude of Rx Meteorological data
Rec. ITU-R P.528	Aeronautical mobile	Point-to-area	Path loss	125 MHz to 15 GHz	0 to 1 800 km (for aeronautical applications 0 km horizontal distance does not mean 0 km path length)	5, 50, 95	Not applicable	H1: 15 m to 20 km H2: 1 to 20 km	Distance Tx height Frequency Rx height Percentage time
Rec. ITU-R P.1146	Land mobile Broadcasting	Point-to-area	Field strength	1 to 3 GHz	1 to 500 km	1 to 99	1 to 99	Tx ≥ 1 m Rx: 1 to 30 m	Distance Frequency Tx antenna height Rx antenna height Percentage time Percentage location Terrain information

Table 1 – ITU-R radiowave propagation prediction methods *(continued)*

Method	Application	Type	Output	Frequency	Distance	% time	% location	Terminal height	Input data
Rec. ITU-R P.529	Land mobile	Point-to-area	Field strength	30 MHz to 3 GHz (limited application above 1.5 GHz)	VHF: 10 to 600 km UHF: 1 to 100 km	VHF: 1, 10, 50 UHF: 50	Unspecified	Base: 20 m to 1 km Mobile: 1 to 10 m	Distance Base antenna height Frequency Mobile antenna height Percentage time Ground cover
Rec. ITU-R P.530	Line-of-sight Fixed links	Point-to-point Line-of-sight	Path loss Diversity improvement (clear air conditions) XPD Outage Error performance	Approximately 150 MHz to 40 GHz	Up to 200 km if line-of-sight	All percentages of time in clear-air conditions; 1 to 0.001 in precipitation conditions [(1)]	Not applicable	High enough to ensure specified path clearance	Distance Tx height Frequency Rx height Percentage time Path obstruction data Climate data
Rec. ITU-R P.533	Broadcasting Fixed Mobile	Point-to-point	Basic MUF Sky-wave field strength Available receiver power Signal-to-noise ratio LUF Circuit reliability	2 to 30 MHz	0 to 40 000 km	All percentages	Not applicable	Not applicable	Latitude and longitude of Tx Latitude and longitude of Rx Sunspot number Month Time(s) of day Frequencies Tx power Tx antenna type Rx antenna type
Rec. ITU-R P.534	Fixed Mobile Broadcasting	Point-to-point via sporadic E	Field strength	30 to 100 MHz	0 to 4 000 km	0 to 50	Not applicable	Not applicable	Distance Frequency
Rec. ITU-R P.616	Maritime mobile	As for Recommendation ITU-R P.370							
Rec. ITU-R P.617	Trans-horizon fixed links	Point-to-point	Path loss	> 30 MHz	100 to 1 000 km	20, 50, 90, 99, and 99.9	Not applicable	No limits specified	Frequency Tx antenna gain Rx antenna gain Path geometry
Rec. ITU-R P.618	Fixed satellite	Point-to-point	Path loss. Diversity gain and (for precipitation condition) XPD	1 to 55 GHz	Any practical orbit height	0.001-5 for attenuation; 0.001-1 for XPD	Not applicable	No limit	Meteorological data Frequency Elevation angle Height of earth station Separation and angle between earth station sites (for diversity gain) Antenna diameter and efficiency (for scintillation) Polarization angle (for XPD)

Table 1 – ITU-R radiowave propagation prediction methods *(end)*

Method	Application	Type	Output	Frequency	Distance	% time	% location	Terminal height	Input data
Rec. ITU-R P.620	Earth station frequency coordination	Coordination distance	Distance of which the required propagation loss is achieved	100 MHz to 105 GHz	up to 1 200 km	0.001 to 50	Not applicable	No limits specified	Minimum basic transmission loss Frequency Percentage of time Earth-station elevation angle
Rec. ITU-R P.680	Maritime mobile satellite	Point-to-point	Sea-surface fading Fade duration Interference (adjacent satellite)	0.8-8 GHz	Any practical orbit height	To 0.001% via Rice-Nakagami distribution Limit of 0.01% for interference(1)	Not applicable	No limit	Frequency Elevation angle Maximum antenna boresight gain
Rec. ITU-R P.681	Land mobile satellite	Point-to-point	Path fading Fade duration Non-fade duration	0.8 to 20 GHz	Any practical orbit height	Not applicable Percentage of distance travelled 1 to 80%(1)	Not applicable	No limit	Frequency Elevation angle Percentage of distance travelled Approximate level of optical shadowing
Rec. ITU-R P.682	Aeronautical mobile satellite	Point-to-point	Sea-surface fading	1 to 2 GHz	Any practical orbit height	To 0.001% via Rice-Nakagami distribution(1)	Not applicable	No limit	Frequency Elevation angle Polarization Maximum antenna boresight gain Antenna height
Rec. ITU-R P.684	Fixed	Point-to-point	Sky-wave field strength	30 to 500 kHz	0 to 40 000 km	50	Not applicable	Not applicable	Latitude and longitude of Tx Latitude and longitude of Rx Distance Tx power Frequency
Rec. ITU-R P.843	Fixed Mobile Broadcasting	Point-to-point via meteor-burst	Received power Burst rate	30 to 100 MHz	100 to 1 000 km	0 to 5	Not applicable	Not applicable	Frequency Distance Tx power Antenna gains

(1) Time percentage of outage; for service availability, subtract value from 100.

APPENDICES

Editor's Note: Texts for information, as adopted by the Intergovernmental Conference on Emergency Telecommunications (ICET-98). The official publication of the Tampere Convention in the United Nations Treaty Series is available, in all six official languages.

TAMPERE CONVENTION ON THE PROVISION OF TELECOMMUNICATION RESOURCES FOR DISASTER MITIGATION AND RELIEF OPERATIONS

THE STATES PARTIES TO THIS CONVENTION,

Recognizing

that the magnitude, complexity, frequency and impact of disasters are increasing at a dramatic rate, with particularly severe consequences in developing countries,

recalling

that humanitarian relief and assistance agencies require reliable, flexible telecommunication resources to perform their vital tasks,

further recalling

the essential role of telecommunication resources in facilitating the safety of humanitarian relief and assistance personnel,

further recalling

the vital role of broadcasting in disseminating accurate disaster information to at-risk populations,

convinced

that the effective, timely deployment of telecommunication resources and that rapid, efficient, accurate and truthful information flows are essential to reducing loss of life, human suffering and damage to property and the environment caused by disasters,

concerned

about the impact of disasters on communication facilities and information flows,

aware

of the special needs of the disaster-prone least developed countries for technical assistance to develop telecommunication resources for disaster mitigation and relief operations,

reaffirming

the absolute priority accorded emergency life-saving communications in more than fifty international regulatory instruments, including the Constitution of the International Telecommunication Union,

noting

the history of international cooperation and coordination in disaster mitigation and relief, including the demonstrated life-saving role played by the timely deployment and use of telecommunication resources,

further noting

the Proceedings of the International Conference on Disaster Communications (Geneva, 1990), addressing the power of telecommunication systems in disaster recovery and response, *further noting*

the urgent call found in the Tampere Declaration on Disaster Communications (Tampere, 1991) for reliable telecommunication systems for disaster mitigation and disaster relief operations, and for an international Convention on Disaster Communications to facilitate such systems,

further noting

United Nations General Assembly Resolution 44/236, designating 1990-2000 the International Decade for Natural Disaster Reduction, and Resolution 46/182, calling for strengthened international coordination of humanitarian emergency assistance,

further noting

the prominent role given to communication resources in the Yokohama Strategy and Plan of Action for a Safer World, adopted by the World Conference on Natural Disaster Reduction (Yokohama, 1994),

further noting

Resolution 7 of the World Telecommunication Development Conference (Buenos Aires, 1994), endorsed by Resolution 36 of the Plenipotentiary Conference of the International Telecommunication Union (Kyoto, 1994), urging governments to take all practical steps for facilitating the rapid deployment and the effective use of telecommunication equipment for disaster mitigation and relief operations by reducing and, where possible, removing regulatory barriers and strengthening cooperation among States,

further noting

Resolution 644 of the World Radiocommunication Conference (Geneva, 1997), urging governments to give their full support to the adoption of this Convention and to its national implementation,

further noting

Resolution 19 of the World Telecommunication Development Conference (Valletta, 1998), urging governments to continue their examination of this Convention with a view to considering giving their full support to its adoption,

further noting

United Nations General Assembly Resolution 51/194, encouraging the development of a transparent and timely procedure for implementing effective disaster relief coordination arrangements, and of ReliefWeb as the global information system for the dissemination of reliable and timely information on emergencies and natural disasters,

with reference

to the conclusions of the Working Group on Emergency Telecommunications regarding the critical role of Telecommunications in disaster mitigation and relief,

supported

by the work of many States, United Nations entities, governmental, intergovernmental, and non-governmental organizations, humanitarian agencies, telecommunication equipment and service providers, media, universities and communication- and disaster-related organizations to improve and facilitate disaster-related communications, *desiring*

to ensure the reliable, rapid availability of telecommunication resources for disaster mitigation and relief operations, and

further desiring

to facilitate international cooperation to mitigate the impact of disasters,

have agreed as follows:

ARTICLE 1

Definitions

Unless otherwise indicated by the context in which they are used, the terms set out below shall have the following meanings for the purposes of this Convention:

1 "State Party" means a State which has agreed to be bound by this Convention.

2 "Assisting State Party" means a State Party to this Convention providing telecommunication assistance pursuant hereto.

3 "Requesting State Party" means a State Party to this Convention requesting telecommunication assistance pursuant hereto.

4 "This Convention" means the Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations.

5 "The depositary" means the depositary for this Convention, as set forth in Article 16.

6 "Disaster" means a serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as the result of complex, long-term processes.

7 "Disaster mitigation" means measures designed to prevent, predict, prepare for, respond to, monitor and/or mitigate the impact of, disasters.

8 "Health hazard" means a sudden outbreak of infectious disease, such as an epidemic or pandemic, or other event posing a significant threat to human life or health, which has the potential for triggering a disaster.

9 "Natural hazard" means an event or process, such as an earthquake, fire, flood, wind, landslide, avalanche, cyclone, tsunami, insect infestation, drought or volcanic eruption, which has the potential for triggering a disaster.

10 "Non-governmental organization" means any organization, including private and corporate entities, other than a State or governmental or intergovernmental organization, concerned with disaster mitigation and relief and/or the provision of telecommunication resources for disaster mitigation and relief.

11 "Non-State entity" means any entity, other than a State, including non-governmental organizations and the Red Cross and Red Crescent Movement, concerned with disaster mitigation and relief and/or the provision of telecommunication resources for disaster mitigation and relief.

12 “Relief operations” means those activities designed to reduce loss of life, human suffering and damage to property and/or the environment caused by a disaster.

13 “Telecommunication assistance” means the provision of telecommunication resources or other resources or support intended to facilitate the use of telecommunication resources.

14 “Telecommunication resources” means personnel, equipment, materials, information, training, radio-frequency spectrum, network or transmission capacity or other resources necessary to telecommunications.

15 “Telecommunications” means any transmission, emission, or reception of signs, signals, writing, images, sounds or intelligence of any nature, by wire, radio, optical fibre or other electromagnetic system.

ARTICLE 2

Coordination

1 The United Nations Emergency Relief Coordinator shall be the operational coordinator for this Convention and shall execute the responsibilities of the operational coordinator identified in Articles 3, 4, 6, 7, 8, and 9.

2 The operational coordinator shall seek the cooperation of other appropriate United Nations agencies, particularly the International Telecommunication Union, to assist it in fulfilling the objectives of this Convention, and, in particular, those responsibilities identified in Articles 8 and 9, and to provide necessary technical support, consistent with the purposes of those agencies.

3 The responsibilities of the operational coordinator under this Convention shall be limited to coordination activities of an international nature.

ARTICLE 3

General Provisions

1 The States Parties shall cooperate among themselves and with non-State entities and intergovernmental organizations, in accordance with the provisions of this Convention, to facilitate the use of telecommunication resources for disaster mitigation and relief.

2 Such use may include, but is not limited to:

a) the deployment of terrestrial and satellite telecommunication equipment to predict, monitor and provide information concerning natural hazards, health hazards and disasters;

b) the sharing of information about natural hazards, health hazards and disasters among the States Parties and with other States, non-State entities and intergovernmental organizations, and the dissemination of such information to the public, particularly to atrisk communities;

c) the provision of prompt telecommunication assistance to mitigate the impact of a disaster; and

d) the installation and operation of reliable, flexible telecommunication resources to be used by humanitarian relief and assistance organizations.

3 To facilitate such use, the States Parties may conclude additional multinational or bilateral agreements or arrangements.

4 The States Parties request the operational coordinator, in consultation with the International Telecommunication Union, the depositary, and other relevant United Nations entities and intergovernmental and non-governmental organizations, to use its best efforts, in accordance with the provisions of this Convention, to:

a) develop, in consultation with the States Parties, model agreements that may be used to provide a foundation for multinational or bilateral agreements facilitating the provision of telecommunication resources for disaster mitigation and relief;

b) make available model agreements, best practices and other relevant information to States Parties, other States, non-State entities and intergovernmental organizations concerning the provision of telecommunication resources for disaster mitigation and relief, by electronic means and other appropriate mechanisms;

c) develop, operate, and maintain information collection and dissemination procedures and systems necessary for the implementation of the Convention; and

d) inform States of the terms of this Convention, and to facilitate and support the cooperation among States Parties provided for herein.

5 The States Parties shall cooperate among themselves to improve the ability of governmental organizations, non-State entities and intergovernmental organizations to establish mechanisms for training in the handling and operation of equipment, and instruction courses in the development, design and construction of emergency telecommunication facilities for disaster prevention, monitoring and mitigation.

ARTICLE 4

Provision of telecommunication assistance

1 A State Party requiring telecommunication assistance for disaster mitigation and relief may request such assistance from any other State Party, either directly or through the operational coordinator. If the request is made through the operational coordinator, the operational coordinator shall immediately disseminate this information to all other appropriate States Parties. If the request is made directly to another State Party, the requesting State Party shall inform the operational coordinator as soon as possible.

2 A State Party requesting telecommunication assistance shall specify the scope and type of assistance required and those measures taken pursuant to Articles 5 and 9 of this Convention, and, when practicable, provide the State Party to which the request is directed and/or the operational coordinator with any other information necessary to determine the extent to which such State Party is able to meet the request.

3 Each State Party to which a request for telecommunication assistance is directed, either directly or through the operational coordinator, shall promptly determine and notify the requesting State Party whether it will render the assistance requested, directly or otherwise, and the scope of, and terms, conditions, restrictions and cost, if any, applicable to such assistance.

4 Each State Party determining to provide telecommunication assistance shall so inform the operational coordinator as soon as possible.

5 No telecommunication assistance shall be provided pursuant to this Convention without the consent of the requesting State Party. The requesting State Party shall retain the authority to reject all or part of any telecommunication assistance offered pursuant to this Convention in accordance with the requesting State Party's existing national law and policy.

6 The States Parties recognize the right of requesting States Parties to request telecommunication assistance directly from non-State entities and intergovernmental organizations, and the right of non-State entities and intergovernmental organizations, pursuant to the laws to which they are subject, to provide telecommunication assistance to requesting States Parties pursuant to this Article.

7 A non-State entity or intergovernmental organization may not be a "requesting State Party" and may not request telecommunication assistance under this Convention.

8 Nothing in this Convention shall interfere with the right of a State Party, under its national law, to direct, control, coordinate and supervise telecommunication assistance provided under this Convention within its territory.

ARTICLE 5

Privileges, Immunities, and Facilities

1 The requesting State Party shall, to the extent permitted by its national law, afford to persons, other than its nationals, and to organizations, other than those headquartered or domiciled within its territory, who act pursuant to this Convention to provide telecommunication assistance and who have been notified to, and accepted by, the requesting State Party, the necessary privileges, immunities, and facilities for the performance of their proper functions, including, but not limited to:

a) immunity from arrest, detention and legal process, including criminal, civil and administrative jurisdiction of the requesting State Party, in respect of acts or omissions specifically and directly related to the provision of telecommunication assistance;

b) exemption from taxation, duties or other charges, except for those which are normally incorporated in the price of goods or services, in respect of the performance of their assistance functions or on the equipment, materials and other property brought into or purchased in the territory of the requesting State Party for the purpose of providing telecommunication assistance under this Convention; and

c) immunity from seizure, attachment or requisition of such equipment, materials and property.

2 The requesting State Party shall provide, to the extent of its capabilities, local facilities and services for the proper and effective administration of the telecommunication assistance, including ensuring that telecommunication equipment brought into its territory pursuant to this Convention shall be expeditiously licensed or shall be exempt from licensing in accordance with its domestic laws and regulations.

3 The requesting State Party shall ensure the protection of personnel, equipment and materials brought into its territory pursuant to this Convention.

4 Ownership of equipment and materials provided pursuant to this Convention shall be unaffected by their use under the terms of this Convention. The requesting State Party shall ensure the prompt return of such equipment, material and property to the proper assisting State Party.

5 The requesting State Party shall not direct the deployment or use of any telecommunication resources provided pursuant to this Convention for purposes not directly related to predicting, preparing for, responding to, monitoring, mitigating the impact of or providing relief during and following disasters.

6 Nothing in this Article shall require any requesting State Party to provide its nationals or permanent residents, or organizations headquartered or domiciled within its territory, with privileges and immunities.

7 Without prejudice to their privileges and immunities in accordance with this Article, all persons entering the territory of a State Party for the purpose of providing telecommunication assistance or otherwise facilitating the use of telecommunication resources pursuant to this Convention, and all organizations providing telecommunication assistance or otherwise facilitating the use of telecommunication resources pursuant to this Convention, have a duty to respect the laws and regulations of that State Party. Such persons and organizations also shall have a duty not to interfere in the domestic affairs of the State Party into whose territory they have entered.

8 Nothing in this Article shall prejudice the rights and obligations with respect to privileges and immunities afforded to persons and organizations participating directly or indirectly in telecommunication assistance, pursuant to other international agreements (including the Convention on the Privileges and Immunities of the United Nations, adopted by the General Assembly on 13 February 1946, and the Convention on the Privileges and Immunities of the Specialized Agencies, adopted by the General Assembly on 21 November 1947) or international law.

ARTICLE 6

Termination of Assistance

1 The requesting State Party or the assisting State Party may, at any time, terminate telecommunication assistance received or provided under Article 4 by providing notification in writing. Upon such notification, the States Parties involved shall consult with each other to provide for the proper and expeditious conclusion of the assistance, bearing in mind the impact of such termination on the risk to human life and ongoing disaster relief operations.

2 States Parties engaged in providing or receiving telecommunication assistance pursuant to this Convention shall remain subject to the terms of this Convention following the termination of such assistance.

3 Any State Party requesting termination of telecommunication assistance shall notify the operational coordinator of such request. The operational coordinator shall provide such assistance as is requested and necessary to facilitate the conclusion of the telecommunication assistance.

ARTICLE 7

Payment or Reimbursement of Costs or Fees

1 The States Parties may condition the provision of telecommunication assistance for disaster mitigation relief upon agreement to pay or reimburse specified costs or fees, always bearing in mind the contents of paragraph 8 of this Article.

2 When such condition exists, the States Parties shall set forth in writing, prior to the provision of telecommunication assistance:

a) the requirement for payment or reimbursement;

b) the amount of such payment or reimbursement or terms under which it shall be calculated; and

c) any other terms, conditions or restrictions applicable to such payment or reimbursement, including, but not limited to, the currency in which such payment or reimbursement shall be made.

3 The requirements of paragraphs 2 b) and 2 c) of this Article may be satisfied by reference to published tariffs, rates or prices.

4 In order that the negotiation of payment and reimbursement agreements does not unduly delay the provision of telecommunication assistance, the operational coordinator shall develop, in consultation with the States Parties, a model payment and reimbursement agreement that may provide a foundation for the negotiation of payment and reimbursement obligations under this Article.

5 No State Party shall be obligated to make payment or reimbursement of costs or fees under this Convention without having first expressed its consent to the terms provided by an assisting State Party pursuant to paragraph 2 of this Article.

6 When the provision of telecommunication assistance is properly conditioned upon payment or reimbursement of costs or fees under this Article, such payment or reimbursement shall be provided promptly after the assisting State Party has presented its request for payment or reimbursement.

7 Funds paid or reimbursed by a requesting State Party in association with the provision of telecommunication assistance shall be freely transferable out of the jurisdiction of the requesting State Party and shall not be delayed or withheld.

8 In determining whether to condition the provision of telecommunication assistance upon an agreement to pay or reimburse specified costs or fees, the amount of such costs or fees, and the terms, conditions and restrictions associated with their payment or reimbursement, the States Parties shall take into account, among other relevant factors:

a) United Nations principles concerning humanitarian assistance;

b) the nature of the disaster, natural hazard or health hazard;

c) the impact, or potential impact, of the disaster;

d) the place of origin of the disaster;

e) the area affected, or potentially affected, by the disaster;

f) the occurrence of previous disasters and the likelihood of future disasters in the affected area;

g) the capacity of each State affected by the disaster, natural hazard or health hazard to prepare for, or respond to, such event; and

h) the needs of developing countries.

9 This Article shall also apply to those situations in which telecommunication assistance is provided by a non-State entity or intergovernmental organization, provided that:

a) the requesting State Party has consented to, and has not terminated, such provision of telecommunication assistance for disaster mitigation and relief;

b) the non-State entity or intergovernmental organization providing such telecommunication assistance has notified to the requesting State Party its adherence to this Article and Articles 4 and 5; and

c) the application of this Article is not inconsistent with any other agreement concerning the relations between the requesting State Party and the non-State entity or intergovernmental organization providing such telecommunication assistance.

ARTICLE 8

Telecommunication Assistance Information Inventory

1 Each State Party shall notify the operational coordinator of its authority(ies):

a) responsible for matters arising under the terms of this Convention and authorized to request, offer, accept and terminate telecommunication assistance; and

b) competent to identify the governmental, intergovernmental and/or non-governmental resources which could be made available to facilitate the use of telecommunication resources for disaster mitigation and relief, including the provision of telecommunication assistance.

2 Each State Party shall endeavour to inform the operational coordinator promptly of any changes in the information provided pursuant to this Article.

3 The operational coordinator may accept notification from a non-State entity or intergovernmental organization of its procedures for authorization to offer and terminate telecommunication assistance as provided in this Article.

4 A State Party, non-State entity or intergovernmental organization may, at its discretion, include in the material it deposits with the operational coordinator information about specific telecommunication resources and about plans for the use those resources to respond to a request for telecommunication assistance from a requesting State Party.

5 The operational coordinator shall maintain copies of all lists of authorities, and shall expeditiously disseminate such material to the States Parties, to other States, and to appropriate non-State entities and intergovernmental organizations, unless a State Party, non-State entity or intergovernmental organization has previously specified, in writing, that distribution of its material be restricted.

6 The operational coordinator shall treat material deposited by non-State entities and intergovernmental organizations in a similar manner to material deposited by States Parties.

ARTICLE 9

Regulatory Barriers

1 The States Parties shall, when possible, and in conformity with their national law, reduce or remove regulatory barriers to the use of telecommunication resources for disaster mitigation and relief, including to the provision of telecommunication assistance.

2 Regulatory barriers may include, but are not limited to:

a) regulations restricting the import or export of telecommunication equipment;

b) regulations restricting the use of telecommunication equipment or of radio-frequency spectrum;

c) regulations restricting the movement of personnel who operate telecommunication equipment or who are essential to its effective use;

d) regulations restricting the transit of telecommunication resources into, out of and through the territory of a State Party; and

e) delays in the administration of such regulations.

3 Reduction of regulatory barriers may take the form of, but shall not be limited to:

a) revising regulations;

b) exempting specified telecommunication resources from the application of those regulations during the use of such resources for disaster mitigation and relief;

c) pre-clearance of telecommunication resources for use in disaster mitigation and relief, in compliance with those regulations;

d) recognition of foreign type-approval of telecommunication equipment and/or operating licenses;

e) expedited review of telecommunication resources for use in disaster mitigation and relief, in compliance with those regulations; and

f) temporary waiver of those regulations for the use of telecommunication resources for disaster mitigation and relief.

4 Each State Party shall, at the request of any other State Party, and to the extent permitted by its national law, facilitate the transit into, out of and through its territory of personnel, equipment, materials and information involved in the use of telecommunication resources for disaster mitigation and relief.

5 Each State Party shall notify the operational coordinator and the other States Parties, directly or through the operational coordinator, of:

a) measures taken, pursuant to this Convention, for reducing or removing such regulatory barriers;

b) procedures available, pursuant to this Convention, to States Parties, other States, non-State entities and/or intergovernmental organizations for the exemption of specified telecommunication resources used for disaster mitigation and relief from the application of such regulations, pre-clearance or expedited review of such resources in compliance with applicable regulations, acceptance of foreign type-approval of such resources, or temporary waiver of regulations otherwise applicable to such resources; and

c) the terms, conditions and restrictions, if any, associated with the use of such procedures.

6 The operational coordinator shall regularly and expeditiously make available to the States Parties, to other States, to non-State entities and to intergovernmental organizations an up-to-date listing of such measures, their scope, and the terms, conditions and restrictions, if any, associated with their use.

7 Nothing in this Article shall permit the violation or abrogation of obligations and responsibilities imposed by national law, international law, or multilateral or bilateral agreements, including obligations and responsibilities concerning customs and export controls.

ARTICLE 10

Relationship to Other International Agreements

1 This Convention shall not affect the rights and obligations of States Parties deriving from other international agreements or international law.

ARTICLE 11

Dispute Settlement

1 In the event of a dispute between States Parties concerning the interpretation or application of this Convention, the States Parties to the dispute shall consult each other for the purpose of settling the dispute. Such consultation shall begin promptly upon the written declaration, delivered by one State Party to another State Party, of the existence of a dispute under this Convention. The State Party making such a written declaration of the existence of a dispute shall promptly deliver a copy of such declaration to the depositary.

2 If a dispute between States Parties cannot be settled within six (6) months of the date of delivery of the written declaration to a State Party to the dispute, the States Parties to the dispute may request any other State Party, State, non-State entity or intergovernmental organization to use its good offices to facilitate settlement of the dispute.

3 If neither State Party seeks the good offices of another State Party, State, non-State entity or intergovernmental organization, or if the exercise of good offices fails to facilitate a settlement of the dispute within six (6) months of the request for such good offices being made, then either State Party to the dispute may:

a) request that the dispute be submitted to binding arbitration; or

b) submit the dispute to the International Court of Justice for decision, provided that both States Parties to the dispute have, at the time of signing, ratifying or acceding to this Convention, or at any time thereafter, accepted the jurisdiction of the International Court of Justice in respect of such disputes.

4 In the event that the respective States Parties to the dispute request that the dispute be submitted to binding arbitration and submit the dispute to the International Court of Justice for decision, the submission to the International Court of Justice shall have priority.

5 In the case of a dispute between a State Party requesting telecommunication assistance and a non-State entity or intergovernmental organization headquartered or domiciled outside of the territory of that State Party concerning the provision of telecommunication assistance under Article 4, the claim of the non-State entity or intergovernmental organization may be espoused directly by the State Party in which the non-State entity or intergovernmental organization is headquartered or domiciled as a State-to-State claim under this Article, provided that such espousal is not inconsistent with any other agreement between the State Party and the non-State entity or intergovernmental organization involved in the dispute.

6 When signing, ratifying, accepting, approving or acceding to this Convention, a State may declare that it does not consider itself bound by either or both of the dispute settlement procedures provided for in paragraph 3 above. The other States Parties shall not be bound by a dispute settlement procedure provided for in paragraph 3 with respect to a State Party for which such a declaration is in force.

ARTICLE 12

Entry into Force

1 This Convention shall be open for signature by all States which are members of the United Nations or of the International Telecommunication Union at the Intergovernmental Conference on Emergency Telecommunications in Tampere on 18 June 1998, and thereafter at the headquarters of the United Nations, New York, from 22 June 1998 to 21 June 2003.

2 A State may express its consent to be bound by this Convention:

a) by signature (definitive signature);

b) by signature subject to ratification, acceptance or approval followed by deposit of an instrument of ratification, acceptance or approval; or

c) by deposit of an instrument of accession.

3 The Convention shall enter into force thirty (30) days after the deposit of instruments of ratification, acceptance, approval or accession or definitive signature of thirty (30) States.

4 For each State which signs definitively or deposits an instrument of ratification, acceptance, approval or accession, after the requirement set out in paragraph 3 of this Article has been fulfilled, this Convention shall enter into force thirty (30) days after the date of the definitive signature or consent to be bound.

ARTICLE 13

Amendments

1 A State Party may propose amendments to this Convention by submitting such amendments to the depositary, which shall circulate them to the other States Parties for approval.

2 The States Parties shall notify the depositary of their approval or disapproval of such proposed amendments within one hundred and eighty (180) days of their receipt.

3 Any amendment approved by two-thirds of all States Parties shall be laid down in a Protocol which is open for signature at the depositary by all States Parties.

4 The Protocol shall enter into force in the same manner as this Convention. For each State which signs the Protocol definitively or deposits an instrument of ratification, acceptance, approval or accession, after the requirements for the entry into force of the Protocol have been fulfilled, the Protocol shall enter into force for such State thirty (30) days after the date of the definitive signature or consent to be bound.

ARTICLE 14

Reservations

1 When definitively signing, ratifying or acceding to this Convention or any amendment hereto, a State Party may make reservations.

2 A State Party may at any time withdraw its prior reservation by written notification to the depositary. Such withdrawal of a reservation becomes effective immediately upon notification to the depositary.

ARTICLE 15

Denunciation

1 A State Party may denounce this Convention by written notification to the depositary.

2 Denunciation shall take effect ninety (90) days following the date of deposit of the written notification.

3 At the request of the denouncing State Party, all copies of the lists of authorities and of measures adopted and procedures available for reducing regulatory measures provided by any State Party denouncing this Convention shall be removed from use by the effective date of such denunciation.

ARTICLE 16

Depositary

1 The Secretary-General of the United Nations shall be the depositary of this Convention.

ARTICLE 17

Authentic Texts

1 The original of this Convention, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the depositary. Only the English, French and Spanish authentic texts will be made available for signature at Tampere on 18 June 1998. The depositary shall prepare the authentic texts in Arabic, Chinese and Russian as soon as possible thereafter.

RESOLUTION 34 (Rev.Doha, 2006)

The role of telecommunications/information and communication technology in early warning and mitigation of disasters and humanitarian assistance

The World Telecommunication Development Conference (Doha, 2006),

recalling

Resolution 34 (Istanbul, 2002) and Recommendation 12 (Istanbul, 2002) of the World Telecommunication Development Conference (WTDC),

considering

a) that the Intergovernmental Conference on Emergency Telecommunications (Tampere, 1998) (ICET-98) adopted the Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations (Tampere Convention) and that this convention came into force in January 2005;

b) that the second Tampere Conference on Disaster Communications (Tampere, 2001) (CDC-01) invited ITU to study the use of public mobile networks for early warning and the dissemination of emergency information and the operational aspects of emergency telecommunications such as call prioritization;

c) that the World Radiocommunication Conference (Geneva, 2003) in its Resolution 646 encouraged administrations to satisfy temporary needs for frequencies in emergency and disaster relief situations, to utilize both existing and new technologies for public protection and disaster relief and to facilitate cross-border circulation of radiocommunication equipment intended for use in emergency and disaster relief situations through mutual cooperation and consultation without hindering national legislation;

d) the potential of modern telecommunication technology as a basic tool for disaster mitigation and relief;

e) the terrible disasters from which many countries suffer, in particular the tsunami disaster that struck many developing countries;

f) that the next international conference on emergency communications 2006 (ICEC-2006) will be held in Tampere, Finland, 19-20 June 2006,

noting

a) that activities are being undertaken at the international, regional and national levels within ITU and other relevant organizations to establish internationally agreed means to operate systems for public protection and disaster relief on a harmonized and coordinated basis;

b) that the capability and flexibility of all telecommunication facilities depend upon appropriate planning for the continuity of each phase of network development and implementation,

further noting

the latest version of the ITU Telecommunication Development Sector (ITU-D) Handbook on Disaster Communications and the adoption of Recommendation ITU-D 13 (Rev.2005) on “Effective utilization of the amateur services in disaster mitigation and relief operations”, *recognizing*

that the recent tragic events in the world clearly demonstrate the need for high-quality communications services to assist public safety and disaster relief agencies in minimizing risk to human life and to cover the necessary general public information and communication needs in such situations,

resolves

to invite ITU-D to continue to ensure that proper consideration be given to telecommunications for disaster warning and disaster situations as an element of telecommunication development, including, in close coordination and collaboration with the ITU Radiocommunication Sector (ITU-R) and the ITU Telecommunication Standardization Sector (ITU-T) and other relevant international organizations, by facilitating and encouraging the use of decentralized means of communications that are appropriate and generally available, including those provided by the amateur radio service and satellite and terrestrial network services,

instructs the Director of the Telecommunication Development Bureau

1 to support administrations in their work towards the implementation of this resolution and of the Tampere Convention;

2 to report to the next world telecommunication development conference on the status of implementation of that Convention;

3 to support administrations and regulators in the recommended activities by incorporating appropriate measures during the implementation of the Doha Action Plan,

requests the Secretary-General

to continue to work closely with the office of the United Nations Emergency Relief Coordinator and other relevant external organizations with a view to further increasing the Union's involvement in, and support to, emergency communications, and to report on the outcome of related international conferences and meetings so that the Plenipotentiary Conference (Antalya, 2006) may take any action that it deems necessary,

invites

1 the United Nations Emergency Relief Coordinator and the Working Group on Emergency Telecommunications and the other relevant external organizations or bodies to collaborate closely with ITU in work towards implementing this resolution and the Tampere Convention, and supporting administrations and international and regional telecommunication organizations in the implementation of the convention;

2 administrations to deploy all necessary efforts to persuade telecommunication service providers to make available their infrastructure in the event of disasters;

3 regulators to ensure that disaster mitigation and relief operations include the provision of necessary telecommunications, through national regulatory rules;

4 ITU-D to expedite the study of aspects of telecommunications related to flexibility and continuity in the event of disasters;

5 administrations that have not yet ratified the Tampere Convention to take necessary action do so as appropriate.

RESOLUTION 36 (Rev.Antalya, 2006)

Telecommunications/information and communication technology in the service of humanitarian assistance

The Plenipotentiary Conference of the International Telecommunication Union (Antalya, 2006),

endorsing

a) Resolution 644 (Rev.WRC-2000) of the World Radiocommunication Conference (WRC), on telecommunication resources for disaster mitigation and relief operations;

b*)* Resolution 646 (WRC-03) of WRC, on public protection and disaster relief;

c) Resolution 34 (Rev.Doha, 2006) of the World Telecommunication Development Conference, on the role of telecommunications/information and communication technology (ICT) in early warning and mitigation of disasters and humanitarian assistance;

d) § 91 of the Tunis Agenda for the Information Society adopted by the second phase of the World Summit on the Information Society,

considering

a) that the Intergovernmental Conference on Emergency Telecommunications (Tampere, 1998) adopted the Tampere Convention on the provision of telecommunication resources for disaster mitigation and relief operations, which entered into force on 8 January 2005;

b) that the second Tampere Conference on Disaster Communications (Tampere, 2001) invited ITU to study the use of public mobile networks for early warning and the dissemination of emergency information, and the operational aspects of emergency telecommunications such as call prioritization;

c) that the third Tampere Conference on Disaster Communications (Tampere, 2006) encouraged wider understanding and cooperation between governments on implementation of the Tampere Convention;

d) that the United Nations World Conference on Disaster Reduction (Kobe, Hyogo, 2005) encouraged all States, taking into account their domestic legal requirements, to consider, as appropriate, acceding to, approving or ratifying relevant international legal instruments relating to disaster reduction, such as the Tampere Convention,

recognizing

a) the seriousness and magnitude of potential disasters that may cause dramatic human suffering;

b) that the recent tragic events in the world clearly demonstrate the need for high-quality communications services to assist public-safety and disaster-relief agencies in minimizing risk to human life and to cover the necessary general public information and communication needs in such situations,

convinced

that the unhindered use of telecommunication/ICT equipment and services is indispensable for the provision of effective and appropriate humanitarian assistance, *further convinced*

that the Tampere Convention provides the necessary framework for such use of telecommunication/ICT resources,

resolves to instruct the Secretary-General and the Director of the Telecommunication Development Bureau

1 to work closely with the United Nations Emergency Relief Coordinator to support Member States which so request in their work towards their national accession to the Tampere Convention;

2 to assist Member States which so request with the development of their practical arrangements for implementation of the Tampere Convention, in close collaboration with the United Nations Emergency Relief Coordinator,

invites Member States

to work towards their accession to the Tampere Convention as a matter of priority,

urges Member States Parties to the Tampere Convention

to take all practical steps for the application of the Tampere Convention and to work closely with the operational coordinator as provided for therein.

RESOLUTION 136 (Antalya, 2006)

The use of telecommunications/information and communication technologies for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief

The Plenipotentiary Conference of the International Telecommunication Union (Antalya, 2006),

recalling

a) Resolution 36 (Rev. Antalya, 2006) of the Plenipotentiary Conference, on telecommunications/ information and communication technologies (ICTs) in the service of humanitarian assistance;

b) Resolution 34 (Rev. Doha, 2006) of the World Telecommunication Development Conference (WTDC), on the role of telecommunications/ICT in early warning and mitigation of disasters and humanitarian assistance;

c) Resolution 48 (Doha, 2006) of WTDC, on strengthening cooperation among telecommunication regulators;

d) Resolution 644 (Rev.WRC-2000) of the World Radiocommunication Conference (WRC), on telecommunication resources for disaster mitigation and relief operations;

e) Resolution 646 (WRC-03) of WRC, on public protection and disaster relief;

f) the emergency telecommunication/ICT coordination mechanisms established by the United Nations Office for the Coordination of Humanitarian Affairs,

taking into account

Resolution 60/125 on international cooperation on humanitarian assistance in the field of natural disasters, from relief to development, adopted by the United Nations General Assembly in March 2006,

noting

a) § 51 of the Geneva Declaration of Principles adopted by the World Summit on the Information Society (WSIS), on the use of ICT applications for disaster prevention;

b) § 20 (c) of the Geneva Plan of Action adopted by WSIS, on e-environment, which calls for the establishment of monitoring systems, using ICTs, to forecast and monitor the impact of natural and man-made disasters, particularly in developing countries, least developed countries and small economies;

c) § 30 of the Tunis Commitment adopted by WSIS, on disaster mitigation;

d) § 91 of the Tunis Agenda for the Information Society adopted by WSIS, on disaster reduction;

e) the effective coordination work of the Partnership Coordination Panel for Telecommunication for Disaster Relief and Mitigation, led by the ITU Telecommunication Standardization Sector, *considering*

a) the devastation suffered from disasters around the world, particularly in developing countries that may suffer disproportionately due to a lack of infrastructure and, therefore, have the most to gain from information on the subject of disaster prevention, mitigation and relief efforts;

b) the potential of modern telecommunications/ICTs to facilitate disaster prevention, mitigation and relief efforts;

c) the ongoing cooperation between ITU study groups and other standards development organizations dealing with emergency telecommunications, alert and warning systems,

recognizing

a) the activities being undertaken at the international and regional levels within ITU and other relevant organizations to establish internationally agreed means for the operation of systems for public protection and disaster relief on a harmonized and coordinated basis;

b) the ongoing development by ITU, in coordination with the United Nations and other United Nations specialized agencies, of guidelines for applying the international content standard for all-media public warning in all disaster and emergency situations;

c) the contribution of the private sector in the prevention, mitigation and relief of emergency and disaster situations which is proving to be effective;

d) the need for a common understanding of the network infrastructure components required to provide rapidly installed, interoperable, robust telecommunication capabilities in humanitarian assistance and disaster relief operations;

e) the importance of working towards the establishment of standards-based monitoring and worldwide early-warning systems, based on telecommunications/ICTs, that are linked to national and regional networks and that facilitate emergency disaster response all over the world, particularly in high-risk regions;

f) the role that the ITU Telecommunication Development Sector can play, through such means as the Global Symposium for Regulators, in collecting and disseminating a set of national regulatory best practices for telecommunication/ICT facilities for disaster prevention, mitigation and relief,

convinced

that an international standard for communication of alert and warning information can assist in the provision of effective and appropriate humanitarian assistance and in mitigating the consequences of disasters, in particular in developing countries,

resolves to instruct the Directors of the Bureaux

1 to continue their technical studies and to develop recommendations, through the ITU study groups, concerning technical and operational implementation, as necessary, of advanced solutions to meet the needs of public protection and disaster relief telecommunications/ICTs, taking into account the capabilities, evolution and any resulting transition requirements of existing systems, particularly those of many developing countries, for national and international operations;

2 to support the development of robust, comprehensive, all-hazards emergency and disaster early-warning, mitigation and relief systems, at national, regional and international levels, including monitoring and management systems involving the use of telecommunications/ICTs (e.g. remote sensing), in collaboration with other international agencies, in order to support coordination at the global and regional level;

3 to promote implementation by appropriate alerting authorities of the international content standard for all-media public warning, in concert with ongoing development of guidelines by all ITU Sectors for application to all disaster and emergency situations;

4 to continue to collaborate with organizations that are working in the area of standards for emergency telecommunications/ICTs and for communication of alert and warning information, in order to study the appropriate inclusion of such standards in ITU's work and their dissemination, in particular in developing countries,

encourages Member States

1 in emergency and disaster relief situations, to satisfy temporary needs for spectrum in addition to what may be normally provided for in agreements with the administrations concerned, while seeking international assistance for spectrum coordination and management, in accordance with the legal framework in force in each country;

2 to work in close collaboration with the Secretary-General, the Directors of the Bureaux, as well as emergency telecommunication/ICT coordination mechanisms of the United Nations, in the development and dissemination of tools, procedures and best practices for the effective coordination and operation of telecommunications/ICTs in disaster situations;

3 to facilitate the use by emergency organizations of both existing and new technologies and solutions (satellite and terrestrial), to the extent practicable, in order to satisfy interoperability requirements and to further the goals of public protection and disaster relief;

4 to develop and support national and regional centres of excellence for research, pre-planning, equipment pre-positioning and deployment of telecommunication/ICT resources for humanitarian assistance and disaster relief coordination,

invites the Secretary-General

to inform the United Nations and, in particular the United Nations Office for the Coordination of Humanitarian Affairs, of this resolution.

Website

www.itu.int/itu-D/emergencytelecoms

VOLUME II

ITU-R CONTRIBUTION

TO THE COMPENDIUM OF ITU'S WORK

ON EMERGENCY TELECOMMUNICATIONS

Table of Contents

Page

Foreword

Telecommunications are critical at all phases of disaster management. Aspects of radiocommunication services associated with disasters include, *inter alia*, disaster prediction, detection, alerting and disaster relief. In certain cases, when the "wired" telecommunication infrastructure is significantly or completely destroyed by a disaster, only radiocommunication services can be employed for disaster relief operations.

Two major tasks of ITU-R – ensuring the effective use of the radio-frequency spectrum and studies concerning development of radiocommunication systems – concern all radiocommunication services. Moreover, the Radiocommunication Study Groups carry out studies related to the continuing development of radiocommunication systems used in disaster mitigation/relief operations and these can be found within the work programmes of the Radiocommunication Study Groups.

Disaster phases	Major radiocommunication services involved	Major tasks of radiocommunication services	Studies carried out by Radio-communication Study Groups
Prediction and Detection	– Meteorological services (meteorological aids and meteorological-satellite service) – Earth exploration-satellite service	Weather and climate prediction. Detection and tracking of earthquakes, tsunamis, hurricanes, typhoons, forest fires, oil leaks, etc. Providing warning information	Study Group 7
Alerting	– Amateur services	Receiving and distributing alert messages	Study Group 8
	– Broadcasting services terrestrial and satellite (radio, television, etc.)	Disseminating alert messages and advice to large sections of the public	Study Group 6
	– Fixed services terrestrial and satellite	Delivering alert messages and instructions to telecommunication centres for further dissemination to public	Study Group 9 Study Group 4
	– Mobile services (land, satellite, maritime services, etc.)	Distributing alert messages and advice to individuals	Study Group 8
Relief	– Amateur services	Assisting in organizing relief operations in areas (especially when other services are still not operational)	Study Group 8
	– Broadcasting services terrestrial and satellite (radio, television, etc.)	Coordination of relief activities by disseminating information from relief planning teams to population	Study Group 6
	– Earth exploration-satellite service	Assessment of damage and providing information for planning relief activities	Study Group 7
	– Fixed services terrestrial and satellite	Exchange of information between different teams/groups for planning and coordination relief activities	Study Group 9 Study Group 4
	– Mobile services (land, satellite, maritime services, etc.)	Exchange of information between individuals and/or groups of people involved in relief activities	Study Group 8

ITU-R is also invited to pursue studies on the further identification of suitable frequency bands that could be used on a global/regional basis for public protection and disaster relief (PPDR), as well as on facilitating cross-border circulation of equipment intended for use in emergency and disaster relief situations – the second of these tasks being reinforced by the Tampere Convention on the provision of telecommunication resources for disaster mitigation and relief operations. Impetus for the work also comes from several Resolutions of World Radiocommunication Conferences (**Resolution 644 (WRC-2000)**, **Resolution 646 (WRC-03)**) requesting ITU-R to study aspects of radiocommunications relevant to disaster mitigation and relief operations.

Introduction

Activities in ITU-R concerning radiocommunications for emergency and disaster relief

1 Background

Studies on radiocommunications for emergency situations and for ensuring safety of life represent a major responsibility of the ITU Radiocommunication Sector. The Radio Regulations (RR) contain numerous provisions for those services associated with distress and safety communications, such as the maritime, aeronautical and radiodetermination services. In addition, there exist many texts (ITU-R Recommendations, Reports, Handbooks) developed by the Radiocommunication Study Groups that have a direct bearing on prediction, detection and radiocommunications relating to disasters and emergencies. These address aspects of spectrum management, such as the protection of safety services from unwanted emissions, as well as providing information on the technical characteristics, spectrum requirements, channelling plans and operational aspects of systems used by services that play a safety of life role.

Following the tsunami in south-east Asia in December 2004, steps have been taken to promote the importance of studies within the Radiocommunication Study Groups which have a bearing on radio-communications needed in the event of natural disasters. To this end, a letter from the Director, BR, was sent to Study Group Chairmen in February 2005 inviting them to review and stimulate activities in their Study Groups pertaining to the topic with a view to contributing to the global effort focused on mitigating the effects of such events in the future.

A summary of the main activities is given below.

2 Radiocommunication Study Group activities

2.1 Study Group 4 (Fixed-satellite service)

Recommendation ITU-R S.1001 – *Use of systems in the fixed-satellite service in the event of natural disasters and similar emergencies for warning and relief operations* provides guidelines on the use of satellite networks in the event of natural disasters and similar emergencies, providing information about the overall system and terminal design that is suitable for disaster relief telecommunications. The revision contains a new section on the use of small earth stations for relief operation and there is an appendix containing examples of small transportable earth stations and of satellite networks used for emergencies in Italy and Japan. Study Group 4 is seeking further examples from administrations on the use of satellite networks for emergency operations.

2.2 Study Group 6 (Broadcasting services)

The Study Group's initial response was a note to the Director summarizing the means by which the broadcasting-satellite service (BSS) can assist in warning the public of impending disasters and in disseminating information relating to relief operations. This was followed by the approval of Question ITU-R 118/6 – *Broadcasting means for public warning and disaster relief*. In response, the

Study Group developed Recommendation ITU-R BT.1774 on the use of satellite and terrestrial broadcast infrastructures for public warning and disaster relief, the aim of which is to help permit the rapid deployment of equipment and networks currently available in the terrestrial and satellite-broadcasting services. These services can provide means for alerting the public, for informing them of preventive measures and for disseminating information on the coordination of rescue procedures. The Recommendation gives technical guidance on the improved usage of terrestrial and satellite broadcast services in cases of natural disasters.

2.3 Study Group 7 (Science services)

This Study Group addresses those services associated with scientific aspects of the subject. The meteorological aids, meteorological-satellite and Earth exploration-satellite services play a major role in the prediction and detection of disasters and in retrieving and relaying data from monitoring equipment (e.g. tsunami detection and prediction system uses buoys – see Fig. 1) to land-based siren systems. More advanced systems involve remote sensing of the ocean temperature whose variations can be linked with seismic activity.

The systems linked with Study Group 7 are used in activities such as:

- weather forecasting and climate change prediction (using the Global Climate Observing System (GCOS) – see Fig. 2);
- detection and tracking of earthquakes, tsunamis, hurricanes, forest fires, oil leaks, etc;
- providing alerting/warning information;
- damage assessment;
- providing information for planning relief operations.

It is essential that the frequencies allocated to these passive services remain free of interference. In this respect, the last World Radiocommunication Conference (WRC-03) secured several relevant frequency allocations. Likewise, the next WRC, in 2007, will look for extended frequency allocations for several science services that will result in improvements such as increased resolution of satellite imaging of the Earth’s surface, at the same time ensuring that adequate protection is given to passive services from harmful interference from other services.

In support of the further development of the services relevant to the prediction and detection of disasters, as well as supporting the regulatory decisions made at WRCs, Study Group 7 has developed many texts, e.g. ITU-R Recommendations and Reports, that address the technical characteristics of the services concerned, as well as related spectrum issues. Amongst new texts currently in preparation are Recommendations on ground-based meteorological aids systems using optical frequencies, spectrum aspects of active and passive sensors (for example used for meteorological observations, vegetation cover assessment, detection of fires and oil leaks, etc.), data collection and dissemination, and interference mitigation techniques applicable in certain bands used by the Earth exploration-satellite service (see www.itu.int/ITU-R/go/rsg7 for further details). In addition, a Handbook is in preparation on the Earth exploration-satellite service which will complement the already existing Handbook on the use of radio spectrum for meteorology, written in conjunction with the International Maritime Organization (IMO), that also describes modern meteorological systems, tools and methods; (see www.itu.int/pub/R-HDB-45/en).

FIGURE 1

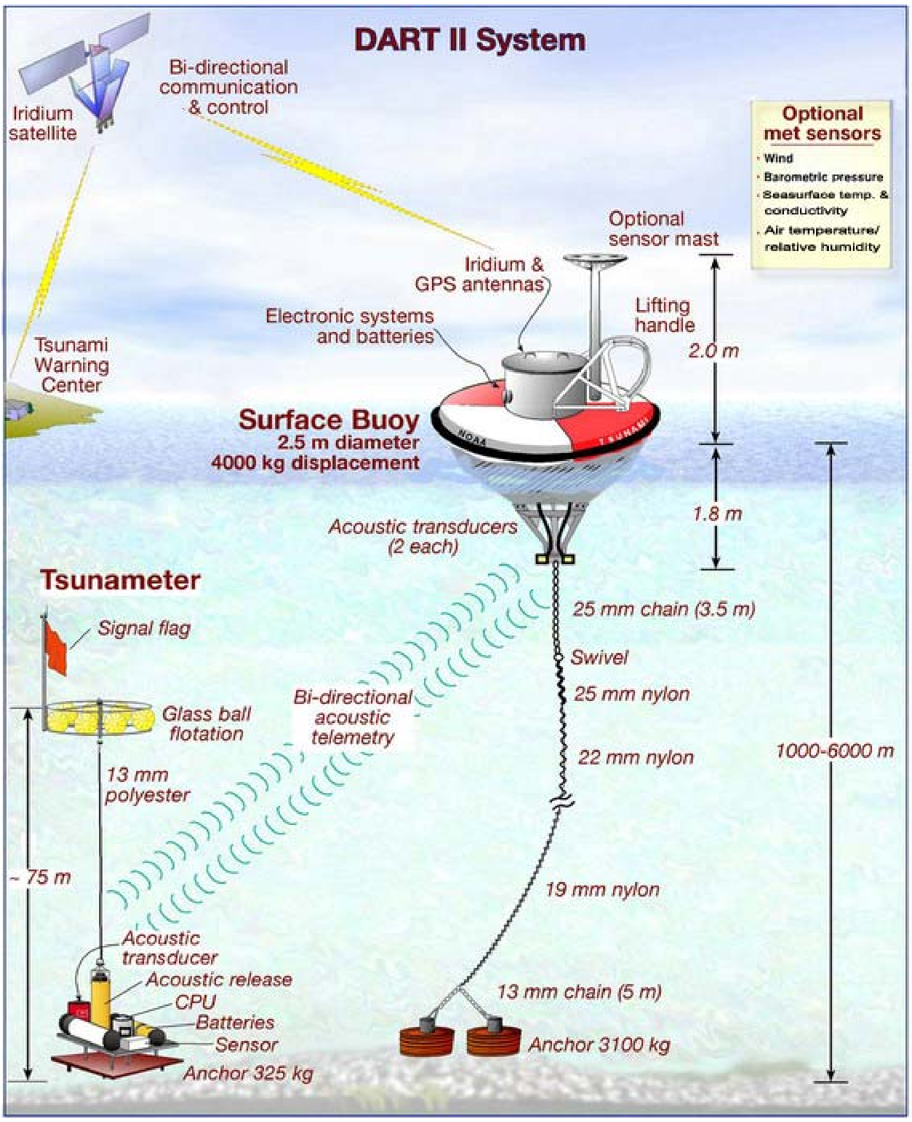
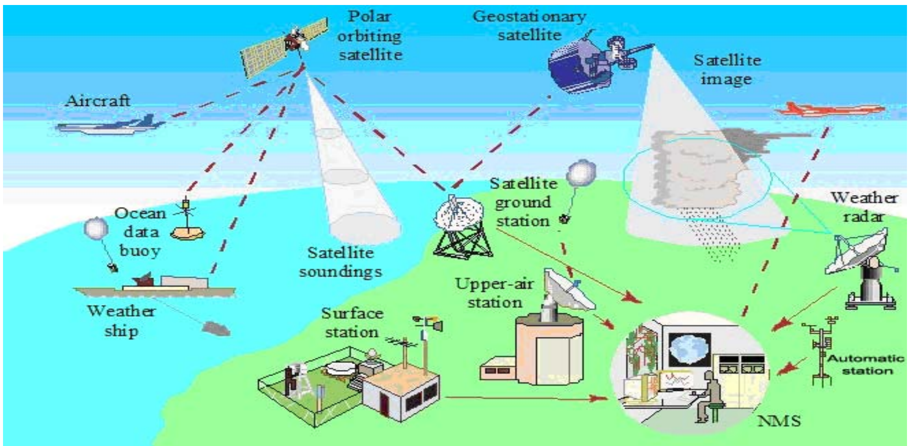


FIGURE 2



2.4 Study Group 8 (Mobile, radiodetermination, amateur and related satellite services)

This Study Group is responsible for many Recommendations that have a bearing on emergency and disaster relief communications. Typically, these provide the technical characteristics of equipment associated with the GMDSS (Global Maritime Distress and Safety System) which include such examples as the transmission characteristics of emergency position-indicating radio beacons (EPIRB) and of a universal shipborne automatic identification system. The Study Group has also been instrumental in studies on PPDR (public protection and disaster relief) and in this respect organized a Workshop on the topic in 2002 (see www.itu.int/ITU-R/study-groups/seminars/rwp8a-protection/). The amateur service has a long history in assisting with radiocommunications during emergencies and disaster events and there are Recommendations developed by Study Group 8 which address the contribution made by amateurs, coupled with that of the land mobile service (see Question ITU-R 209/8).

Much of the work undertaken within the Study Group has been in support of Radio Regulatory texts and procedures addressing distress and safety communications and many relevant provisions exist in Articles of the RR. The subject of frequency bands for PPDR communications was an important item on the agenda of WRC-03. Previously WRC-2000 had adopted two Resolutions (**644 (Rev. WRC-2000)** and **645 (WRC-2000)**) addressing the subject, requesting ITU-R (Study Group 8) to study aspects of radiocommunications relevant to disaster mitigation and relief operations and also to study the question of identifying frequency bands that could be used on a global/regional basis. Report ITU-R M.2033 was prepared in response to those Resolutions.

The result from WRC-03 is reflected in Resolution **646 (WRC-03)** which strongly recommends use of regionally harmonized bands and encourages consideration of the use of certain bands in the three ITU Regions. Studies in this domain continue within Study Group 8 and include, amongst others, the further identification of other frequency ranges suitable for such purposes and the use of mobile-satellite systems for disaster relief.

2.5 Study Group 9 (Fixed service)

Two study Questions address the need for technical and operational characteristics of systems in the fixed service for disaster mitigation and relief, one of the Questions placing particular emphasis on systems operating in the MF/HF bands. At the same time, the Study Group has prepared a significant revision to Recommendation ITU-R F.1105 – *Transportable fixed radiocommunications equipment for relief operations*. This Recommendation updates the characteristics of such fixed wireless systems that are specified according to channel capacity, operating frequencies, transmission distance and propagation path characteristics. The features of a regional digital simultaneous communication system (RDSCS) are described. Such a system can provide simultaneous individual or group communications between a central station and a number of terminals in a region. The central station collects data and information relevant to the prevention phase of a disaster and can then transmit such information to residents for alerting purposes; interactive capabilities are also available.

3 Other activities in BR

3.1 ITU-R website on the role of radiocommunications in disaster mitigation and relief operations

A dedicated website (www.itu.int/ITU-R/index.asp?category=information&link=emergency& lang=en) has been developed, which describes the role that ITU-R plays in disaster mitigation and relief operations. In distinguishing the different phases of a disaster – *prediction, detection, alerting, relief* – the website identifies the radio services involved, their tasks and the relevant Radiocommunication Study Groups involved in studies for providing information and recommendations.

3.2 Additional information concerning the Radiocommunication Sector

3.2.1 Maritime mobile Access and Retrieval System (MARS)

This system has been developed by the International Telecommunication Union (see www.itu.int/ITU-R/terrestrial/mars/) with the purpose of providing the maritime community, in particular those entities that are involved in search and rescue activities, with the most up-to-date data registered in the ITU master Ship station database.

Updated weekly and available on a 24-hour per day/7-day per week basis, this system contains characteristics of over 400 000 ship stations as well as the addresses and contact information for Accounting Authorities (AAICs) and Notifying Administrations.

3.2.2 Regionally harmonized bands

Information referring to these bands can be found in Resolution **646 (WRC-03)** – *Public protection and disaster relief* (see www.itu.int/ITU-R/index.asp?category=information&link=emergency-bands&lang=en).

Annex 1

ITU-R texts concerning radiocommunications for emergency and disaster relief

Index

Section I – Radio Regulations texts

ARTICLE 30

General provisions

Section I – Introduction

30.1 § 1 This Chapter contains the provisions for the operational use of the global maritime distress and safety system (GMDSS), which is fully defined in the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended. Distress, urgency and safety transmissions may also be made, using Morse telegraphy or radiotelephony techniques, in accordance with the provisions of Appendix **13** and relevant ITU-R Recommendations. Stations of the maritime mobile service, when using frequencies and techniques in conformity with Appendix **13**, shall comply with the appropriate provisions of that Appendix.

30.2 § 2 No provision of these Regulations prevents the use by a mobile station or a mobile earth station in distress of any means at its disposal to attract attention, make known its position, and obtain help (see also No. **4.9**).

30.3 § 3 No provision of these Regulations prevents the use by stations on board aircraft, ships engaged in search and rescue operations, land stations, or coast earth stations, in exceptional circumstances, of any means at their disposal to assist a mobile station or a mobile earth station in distress (see also Nos. **4.9** and **4.16**).

Section II – Maritime provisions

30.4 § 4 The provisions specified in this Chapter are obligatory (see Resolution **331 (Rev.WRC-97)**[*]) in the maritime mobile service and the maritime mobile-satellite service for all stations using the frequencies and techniques prescribed for the functions set out herein (see also No. **30.5**). However, stations of the maritime mobile service, when fitted with equipment used by stations operating in conformity with Appendix **13**, shall comply with the appropriate provisions of that Appendix.

30.5 § 5 The International Convention for the Safety of Life at Sea (SOLAS), 1974 as amended, prescribes which ships and which of their survival craft shall be provided with radio equipment, and which ships shall carry portable radio equipment for use in survival craft. It also prescribes the requirements which shall be met by such equipment.

---

[*] *Note by the Secretariat:* This Resolution was revised by WRC-03.

30.6 § 6 Ship earth stations located at rescue coordination centres[1] may be authorized by an administration to communicate for distress and safety purposes with any other station using bands allocated to the maritime mobile-satellite service, when special circumstances make it essential, notwithstanding the methods of working provided for in these Regulations.

30.7 § 7 Mobile stations[2] of the maritime mobile service may communicate, for safety purposes, with stations of the aeronautical mobile service. Such communications shall normally be made on the frequencies authorized, and under the conditions specified in Section I of Article **31** (see also No. **4.9**).

Section III – Aeronautical provisions

30.8 § 8 The procedure specified in this Chapter is obligatory for communications between stations on board aircraft and stations of the maritime mobile-satellite service, wherever this service or stations of this service are specifically mentioned.

30.9 § 9 Certain provisions of this Chapter are applicable to the aeronautical mobile service, except in the case of special arrangements between the governments concerned.

30.10 § 10 Mobile stations of the aeronautical mobile service may communicate, for distress and safety purposes, with stations of the maritime mobile service in conformity with the provisions of this Chapter.

30.11 § 11 Any station on board an aircraft required by national or international regulations to communicate for distress, urgency or safety purposes with stations of the maritime mobile service that comply with the provisions of this Chapter, shall be capable of transmitting and receiving class J3E emissions when using the carrier frequency 2 182 kHz, or class J3E emissions when using the carrier frequency 4 125 kHz, or class G3E emissions when using the frequency 156.8 MHz and, optionally, the frequency 156.3 MHz.

Section IV – Land mobile provisions

30.12 § 12 Stations of the land mobile service in uninhabited, sparsely populated or remote areas may, for distress and safety purposes, use the frequencies provided for in this Chapter.

30.13 § 13 The procedure specified in this Chapter is obligatory for stations of the land mobile service when using frequencies provided in these Regulations for distress and safety communications.

---

[1] **30.6.1** The term "rescue coordination centre", as defined in the International Convention on Maritime Search and Rescue (1979), refers to a unit responsible for promoting the efficient organization of search and rescue services and for coordinating the conduct of search and rescue operations within a search and rescue region.

[2] **30.7.1** Mobile stations communicating with the stations of the aeronautical mobile (R) service in bands allocated to the aeronautical mobile (R) service shall conform to the provisions of the Regulations which relate to that service and, as appropriate, to any special arrangements between the governments concerned by which the aeronautical mobile (R) service is regulated.

ARTICLE 31

Frequencies for the global maritime distress and safety system (GMDSS)

Section I – General

31.1 § 1 The frequencies to be used for the transmission of distress and safety information under the GMDSS are contained in Appendix **15**. In addition to the frequencies listed in Appendix **15**, coast stations should use other appropriate frequencies for the transmission of safety messages.

31.2 § 2 Any emission causing harmful interference to distress and safety communications on any of the discrete frequencies identified in Appendices **13** and **15** is prohibited.

31.3 § 3 The number and duration of test transmissions shall be kept to a minimum on the frequencies identified in Appendix **15**; they should be coordinated with a competent authority, as necessary, and, wherever practicable, be carried out on artificial antennas or with reduced power. However, testing on the distress and safety calling frequencies should be avoided, but where this is unavoidable, it should be indicated that these are test transmissions.

31.4 § 4 Before transmitting for other than distress purposes on any of the frequencies identified in Appendix **15** for distress and safety, a station shall, where practicable, listen on the frequency concerned to make sure that no distress transmission is being sent.

31.5 Not used.

Section II – Survival craft stations

31.6 § 5 1) Equipment for radiotelephony use in survival craft stations shall, if capable of operating on any frequency in the bands between 156 MHz and 174 MHz, be able to transmit and receive on 156.8 MHz and at least one other frequency in these bands.

31.7 2) Equipment for transmitting locating signals from survival craft stations shall be capable of operating in the 9 200-9 500 MHz band.

31.8 3) Equipment with digital selective calling facilities for use in survival craft shall, if capable of operating:

31.9 *a)* in the bands between 1 606.5 kHz and 2 850 kHz, be able to transmit on 2 187.5 kHz; (WRC-03)

31.10 *b)* in the bands between 4 000 kHz and 27 500 kHz, be able to transmit on 8 414.5 kHz;

31.11 *c)* in the bands between 156 MHz and 174 MHz, be able to transmit on 156.525 MHz.

Section III – Watchkeeping

31.12 *A – Coast stations*

31.13 § 6 Those coast stations assuming a watch-keeping responsibility in the GMDSS shall maintain an automatic digital selective calling watch on frequencies and for periods of time as indicated in the information published in the List of Coast Stations.

31.14 *B – Coast earth stations*

31.15 § 7 Those coast earth stations assuming a watch-keeping responsibility in the GMDSS shall maintain a continuous automatic watch for appropriate distress alerts relayed by space stations.

31.16 *C – Ship stations*

31.17 § 8 1) Ship stations, where so equipped, shall, while at sea, maintain an automatic digital selective calling watch on the appropriate distress and safety calling frequencies in the frequency bands in which they are operating. Ship stations, where so equipped, shall also maintain watch on the appropriate frequencies for the automatic reception of transmissions of meteorological and navigational warnings and other urgent information to ships. However, ship stations shall also continue to apply the appropriate watch-keeping provisions of Appendix **13** (see Resolution **331 (Rev.WRC-97)***).

31.18 2) Ship stations complying with the provisions of this Chapter should, where practicable, maintain a watch on the frequency 156.650 MHz for communications related to the safety of navigation.

31.19 *D – Ship earth stations*

31.20 § 9 Ship earth stations complying with the provisions of this Chapter shall, while at sea, maintain watch except when communicating on a working channel.

* *Note by the Secretariat:* This Resolution was revised by WRC-03.

ARTICLE 32

Operational procedures for distress and safety communications in the global maritime distress and safety system (GMDSS)

Section I – General

32.1 § 1 Distress and safety communications rely on the use of terrestrial MF, HF and VHF radiocommunications and communications using satellite techniques.

32.2 § 2 1) The distress alert (see No. **32.9**) shall be sent through a satellite either with absolute priority in general communication channels or on exclusive distress and safety frequencies or, alternatively, on the distress and safety frequencies in the MF, HF and VHF bands using digital selective calling.

32.3 2) The distress alert (see No. **32.9**) shall be sent only on the authority of the person responsible for the ship, aircraft or other vehicle carrying the mobile station or the mobile earth station.

32.4 § 3 All stations which receive a distress alert transmitted by digital selective calling shall immediately cease any transmission capable of interfering with distress traffic and shall continue watch until the call has been acknowledged.

32.5 § 4 Digital selective calling shall be in accordance with the relevant ITU-R Recommendations.

32.5A § 4A Each administration shall ensure that suitable arrangements are made for assigning and registering identities used by ships participating in the GMDSS, and shall make registration information available to rescue coordination centres on a 24-hour day, 7-day week basis. Where appropriate, administrations shall notify responsible organizations immediately of additions, deletions and other changes in these assignments (see Nos. **19.39**, **19.96** and **19.99**). Registration information shall be in accordance with Resolution **340 (WRC-97)**.

32.5B § 4B Any GMDSS shipboard equipment which is capable of transmitting position coordinates as part of a distress alert message and which does not have an integral electronic position-fixing system receiver shall be interconnected to a separate navigation receiver, if one is installed, to provide that information automatically.

32.6 § 5 Transmissions by radiotelephony shall be made slowly and distinctly, each word being clearly pronounced to facilitate transcription.

32.7 § 6 The phonetic alphabet and figure code in Appendix **14** and the abbreviations and signals in accordance with the most recent version of Recommendation ITU-R M.1172 should be used where applicable[1]. (WRC-03)

[1] **32.7.1** The use of the Standard Marine Communication Phrases and, where language difficulties exists, the International Code of Signals, both published by the International Maritime Organization (IMO), is also recommended.

Section II – Distress alerting

32.8 *A – General*

32.9 § 7 1) The transmission of a distress alert indicates that a mobile unit[2] or person[3] is threatened by grave and imminent danger and requests immediate assistance. The distress alert is a digital selective call using a distress call format[4] in the bands used for terrestrial radiocommunication or a distress message format, in which case it is relayed through space stations.

32.10 2) The distress alert shall provide[5] the identification of the station in distress and its position.

32.10A § 7A A distress alert is false if it was transmitted without any indication that a mobile unit or person was in distress and required immediate assistance (see No. **32.9**). Administrations receiving a false distress alert shall report this infringement in accordance with Section V of Article **15**, if that alert:

a) was transmitted intentionally;

b) was not cancelled in accordance with Resolution **349 (WRC-97)**;

c) could not be verified as a result of either the ship's failure to keep watch on appropriate frequencies in accordance with Nos. **31.16** to **31.20**, or its failure to respond to calls from an authorized rescue authority;

d) was repeated; or

e) was transmitted using a false identity.

Administrations receiving such a report shall take appropriate steps to ensure that the infringement does not recur. No action should normally be taken against any ship or mariner for reporting and cancelling a false distress alert.

32.11 *B – Transmission of a distress alert*

B1 – Transmission of a distress alert by a ship station or a ship earth station

32.12 § 8 Ship-to-shore distress alerts are used to alert rescue coordination centres via coast stations or coast earth stations that a ship is in distress. These alerts are based on the use of transmissions via satellites (from a ship earth station or a satellite EPIRB) and terrestrial services (from ship stations and EPIRBs).

32.13 § 9 Ship-to-ship distress alerts are used to alert other ships in the vicinity of the ship in distress and are based on the use of digital selective calling in the VHF and MF bands. Additionally, the HF band may be used.

---

[2] **32.9.1** Mobile unit: a ship, aircraft or other vehicle.

[3] **32.9.2** In this Article, where the case is of a person in distress, the application of the procedures may require adaptation to meet the needs of the particular circumstances.

[4] **32.9.3** The format of distress calls and distress messages shall be in accordance with the relevant ITU-R Recommendations (see Resolution **27 (Rev.WRC-03)**.

[5] **32.10.1** The distress alert may also contain information regarding the nature of the distress, the type of assistance required, the course and speed of the mobile unit, the time that this information was recorded and any other information which might facilitate rescue.

B2 – Transmission of a shore-to-ship distress alert relay

32.14 § 10 1) A station or a rescue coordination centre which receives a distress alert shall initiate the transmission of a shore-to-ship distress alert relay addressed, as appropriate, to all ships, to a selected group of ships or to a specific ship by satellite and/or terrestrial means.

32.15 2) The distress alert relay shall contain the identification of the mobile unit in distress, its position and all other information which might facilitate rescue.

B3 – Transmission of a distress alert by a station not itself in distress

32.16 § 11 A station in the mobile or mobile-satellite service which learns that a mobile unit is in distress shall initiate and transmit a distress alert in any of the following cases:

32.17 *a)* when the mobile unit in distress is not itself in a position to transmit the distress alert;

32.18 *b)* when the master or person responsible for the mobile unit not in distress or the person responsible for the land station considers that further help is necessary.

32.19 § 12 A station transmitting a distress alert relay in accordance with Nos. **32.16**, **32.17**, **32.18** and **32.31** shall indicate that it is not itself in distress.

32.20 *C – Receipt and acknowledgement of distress alerts*

C1 – Procedure for acknowledgement of receipt of distress alerts

32.21 § 13 Acknowledgement by digital selective calling of receipt of a distress alert in the terrestrial services shall be in accordance with relevant ITU-R Recommendations (see Resolution **27 (Rev.WRC-03)**).

32.22 § 14 Acknowledgement through a satellite of receipt of a distress alert from a ship earth station shall be sent immediately (see No. **32.26**).

32.23 § 15 1) Acknowledgement by radiotelephony of receipt of a distress alert from a ship station or a ship earth station shall be given in the following form:

- the distress signal MAYDAY;
- the call sign or other identification of the station sending the distress message, spoken three times;
- the words THIS IS (or DE spoken as DELTA ECHO in case of language difficulties);
- the call sign or other identification of the station acknowledging receipt, spoken three times;
- the word RECEIVED (or RRR spoken as ROMEO ROMEO ROMEO in case of language difficulties);
- the distress signal MAYDAY.

32.24 2) The acknowledgement by direct-printing telegraphy of receipt of a distress alert from a ship station shall be given in the following form:

– the distress signal MAYDAY;

– the call sign or other identification of the station sending the distress alert;

– the word DE;

– the call sign or other identification of the station acknowledging receipt of the distress alert;

– the signal RRR;

– the distress signal MAYDAY.

32.25 § 16 The acknowledgement by direct-printing telegraphy of receipt of a distress alert from a ship earth station shall be given by the coast earth station receiving the distress alert, by retransmitting the ship station identity of the ship transmitting the distress alert.

C2 – Receipt and acknowledgement of receipt by a coast station, a coast earth station or a rescue coordination centre

32.26 § 17 Coast stations and appropriate coast earth stations in receipt of distress alerts shall ensure that they are routed as soon as possible to a rescue coordination centre. Receipt of a distress alert is to be acknowledged as soon as possible by a coast station, or by a rescue coordination centre via a coast station or an appropriate coast earth station.

32.27 § 18 A coast station using digital selective calling to acknowledge a distress call shall transmit the acknowledgement on the distress calling frequency on which the call was received and should address it to all ships. The acknowledgement shall include the identification of the ship whose distress call is being acknowledged.

C3 – Receipt and acknowledgement of receipt by a ship station or ship earth station

32.28 § 19 1) Ship or ship earth stations in receipt of a distress alert shall, as soon as possible, inform the master or person responsible for the ship of the contents of the distress alert.

32.29 2) In areas where reliable communications with one or more coast stations are practicable, ship stations in receipt of a distress alert should defer acknowledgement for a short interval so that receipt may be acknowledged by a coast station.

32.30 § 20 1) Ship stations operating in areas where reliable communications with a coast station are not practicable which receive a distress alert from a ship station which is, beyond doubt, in their vicinity, shall, as soon as possible and if appropriately equipped, acknowledge receipt and inform a rescue coordination centre through a coast station or coast earth station (see No. **32.18**).

32.31 2) However, a ship station receiving an HF distress alert shall not acknowledge it but shall observe the provisions of Nos. **32.36** to **32.38**, and shall, if the alert is not acknowledged by a coast station within 3 minutes, relay the distress alert.

32.32 § 21 A ship station acknowledging receipt of a distress alert in accordance with No. **32.29** or No. **32.30** should:

32.33 *a)* in the first instance, acknowledge receipt of the alert by using radiotelephony on the distress and safety traffic frequency in the band used for the alert;

32.34 *b)* if acknowledgement by radiotelephony of the distress alert received on the MF or VHF distress alerting frequency is unsuccessful, acknowledge receipt of the distress alert by responding with a digital selective call on the appropriate frequency.

32.35 § 22 A ship station in receipt of a shore-to-ship distress alert (see No. **32.14**) should establish communication as directed and render such assistance as required and appropriate.

32.36 *D – Preparations for handling of distress traffic*

32.37 § 23 On receipt of a distress alert transmitted by use of digital selective calling techniques, ship stations and coast stations shall set watch on the radiotelephone distress and safety traffic frequency associated with the distress and safety calling frequency on which the distress alert was received.

32.38 § 24 Coast stations and ship stations with narrow-band direct-printing equipment shall set watch on the narrow-band direct-printing frequency associated with the distress alert signal if it indicates that narrow-band direct-printing is to be used for subsequent distress communications. If practicable, they should additionally set watch on the radiotelephone frequency associated with the distress alert frequency.

Section III – Distress traffic

32.39 *A – General and search and rescue coordinating communications*

32.40 § 25 Distress traffic consists of all messages relating to the immediate assistance required by the ship in distress, including search and rescue communications and on-scene communications. The distress traffic shall as far as possible be on the frequencies contained in Article **31**.

32.41 § 26 1) The distress signal consists of the word MAYDAY, pronounced in radiotelephony as the French expression “m'aider”.

32.42 2) For distress traffic by radiotelephony, when establishing communications, calls shall be prefixed by the distress signal MAYDAY.

32.43 § 27 1) Error correction techniques in accordance with relevant ITU-R Recommendations shall be used for distress traffic by direct-printing telegraphy. All messages shall be preceded by at least one carriage return, a line feed signal, a letter shift signal and the distress signal MAYDAY.

32.44 2) Distress communications by direct-printing telegraphy should normally be established by the ship in distress and should be in the broadcast (forward error correction) mode. The ARQ mode may subsequently be used when it is advantageous to do so.

32.45 § 28 1) The Rescue Coordination Centre responsible for controlling a search and rescue operation shall also coordinate the distress traffic relating to the incident or may appoint another station to do so.

32.46 2) The rescue coordination centre coordinating distress traffic, the unit coordinating search and rescue operations[6] or the coast station involved may impose silence on stations which interfere with that traffic. This instruction shall be addressed to all stations or to one station only, according to circumstances. In either case, the following shall be used:

32.47 *a)* in radiotelephony, the signal SEELONCE MAYDAY, pronounced as the French expression "silence, m'aider";

32.48 *b)* in narrow-band direct-printing telegraphy normally using forward-error correcting mode, the signal SILENCE MAYDAY. However, the ARQ mode may be used when it is advantageous to do so.

32.49 § 29 Until they receive the message indicating that normal working may be resumed (see No. **32.51**), all stations which are aware of the distress traffic, and which are not taking part in it, and which are not in distress, are forbidden to transmit on the frequencies in which the distress traffic is taking place.

32.50 § 30 A station of the mobile service which, while following distress traffic, is able to continue its normal service, may do so when the distress traffic is well established and on condition that it observes the provisions of No. **32.49** and that it does not interfere with distress traffic.

32.51 § 31 When distress traffic has ceased on frequencies which have been used for distress traffic, the rescue coordination centre controlling a search and rescue operation shall initiate a message for transmission on these frequencies indicating that distress traffic has finished.

32.52 § 32 1) In radiotelephony, the message referred to in No. **32.51** consists of:

– the distress signal MAYDAY;
– the call "Hello all stations" or CQ (spoken as CHARLIE QUEBEC) spoken three times;
– the words THIS IS (or DE spoken as DELTA ECHO in the case of language difficulties);
– the call sign or other identification of the station sending the message;
– the time of handing in of the message;
– the name and call sign of the mobile station which was in distress;
– the words SEELONCE FEENEE pronounced as the French words "silence fini".

32.53 2) In direct-printing telegraphy, the message referred to in No. **32.51** consists of:

– the distress signal MAYDAY;
– the call CQ;
– the word DE;
– the call sign or other identification of the station sending the message;
– the time of handing in of the message;
– the name and call sign of the mobile station which was in distress; and
– the words SILENCE FINI.

---

6 **32.46.1** In accordance with the International Convention on Maritime Search and Rescue (1979), this is the on-scene commander (OSC) or the coordinator surface search (CSS).

32.54 *B – On-scene communications*

32.55 § 33 1) On-scene communications are those between the mobile unit in distress and assisting mobile units, and between the mobile units and the unit coordinating search and rescue operations [6].

32.56 2) Control of on-scene communications is the responsibility of the unit coordinating search and rescue operations[6]. Simplex communications shall be used so that all on-scene mobile stations may share relevant information concerning the distress incident. If direct-printing telegraphy is used, it shall be in the forward error-correcting mode.

32.57 § 34 1) The preferred frequencies in radiotelephony for on-scene communications are 156.8 MHz and 2 182 kHz. The frequency 2 174.5 kHz may also be used for ship-to-ship on-scene communications using narrow-band direct-printing telegraphy in the forward error correcting mode.

32.58 2) In addition to 156.8 MHz and 2 182 kHz, the frequencies 3 023 kHz, 4 125 kHz, 5 680 kHz, 123.1 MHz and 156.3 MHz may be used for ship-to-aircraft on-scene communications.

32.59 § 35 The selection or designation of on-scene frequencies is the responsibility of the unit coordinating search and rescue operations[6]. Normally, once an on-scene frequency is established, a continuous aural or teleprinter watch is maintained by all participating on-scene mobile units on the selected frequency.

32.60 *C – Locating and homing signals*

32.61 § 36 1) Locating signals are radio transmissions intended to facilitate the finding of a mobile unit in distress or the location of survivors. These signals include those transmitted by searching units, and those transmitted by the mobile unit in distress, by survival craft, by float-free EPIRBs, by satellite EPIRBs and by search and rescue radar transponders to assist the searching units.

32.62 2) Homing signals are those locating signals which are transmitted by mobile units in distress, or by survival craft, for the purpose of providing searching units with a signal that can be used to determine the bearing to the transmitting stations.

32.63 3) Locating signals may be transmitted in the following frequency bands:

117.975-136 MHz;

156-174 MHz;

406-406.1 MHz;

1 645.5-1 646.5 MHz; and

9 200-9 500 MHz.

32.64 4) Locating signals shall be in accordance with the relevant ITU-R Recommendations (see Resolution **27 (Rev.WRC-03)**).

---

[6] **32.55.1**, **32.56.1** and **32.59.1** In accordance with the International Convention on Maritime Search and Rescue (1979), this is the on-scene commander (OSC) or the coordinator surface search (CSS).

ARTICLE 33

Operational procedures for urgency and safety communications in the global maritime distress and safety system (GMDSS)

Section I – General

33.1 § 1 Urgency and safety communications include:

33.2 *a)* navigational and meteorological warnings and urgent information;

33.3 *b)* ship-to-ship safety of navigation communications;

33.4 *c)* ship reporting communications;

33.5 *d)* support communications for search and rescue operations;

33.6 *e)* other urgency and safety messages; and

33.7 *f)* communications relating to the navigation, movements and needs of ships and weather observation messages destined for an official meteorological service.

Section II – Urgency communications

33.8 § 2 In a terrestrial system the announcement of the urgency message shall be made on one or more of the distress and safety calling frequencies specified in Section I of Article **31** using digital selective calling and the urgency call format. A separate announcement need not be made if the urgency message is to be transmitted through the maritime mobile-satellite service.

33.9 § 3 The urgency signal and message shall be transmitted on one or more of the distress and safety traffic frequencies specified in Section I of Article **31**, or via the maritime mobile-satellite service or on other frequencies used for this purpose.

33.10 § 4 The urgency signal consists of the words PAN PAN. In radiotelephony each word of the group shall be pronounced as the French word "panne".

33.11 § 5 The urgency call format and the urgency signal indicate that the calling station has a very urgent message to transmit concerning the safety of a mobile unit or a person.

33.12 § 6 1) In radiotelephony, the urgency message shall be preceded by the urgency signal (see No. **33.10**), repeated three times, and the identification of the transmitting station.

33.13 2) In narrow-band direct-printing, the urgency message shall be preceded by the urgency signal (see No. **33.10**) and the identification of the transmitting station.

33.14 § 7 1) The urgency call format or urgency signal shall be sent only on the authority of the master or the person responsible for the mobile unit carrying the mobile station or mobile earth station.

33.15 2) The urgency call format or the urgency signal may be transmitted by a land station or a coast earth station with the approval of the responsible authority.

33.16 § 8 When an urgency message which calls for action by the stations receiving the message has been transmitted, the station responsible for its transmission shall cancel it as soon as it knows that action is no longer necessary.

33.17 § 9 1) Error correction techniques in accordance with relevant ITU-R Recommendations shall be used for urgency messages by direct-printing telegraphy. All messages shall be preceded by at least one carriage return, a line feed signal, a letter shift signal and the urgency signal PAN PAN.

33.18 2) Urgency communications by direct-printing telegraphy should normally be established in the broadcast (forward error correction) mode. The ARQ mode may subsequently be used when it is advantageous to do so.

Section III – Medical transports

33.19 § 10 The term "medical transports", as defined in the 1949 Geneva Conventions and Additional Protocols, refers to any means of transportation by land, water or air, whether military or civilian, permanent or temporary, assigned exclusively to medical transportation and under the control of a competent authority of a party to a conflict or of neutral States and of other States not parties to an armed conflict, when these ships, craft and aircraft assist the wounded, the sick and the shipwrecked.

33.20 § 11 For the purpose of announcing and identifying medical transports which are protected under the above-mentioned Conventions, the procedure of Section II of this Article is used. The urgency signal shall be followed by the addition of the single word MEDICAL in narrow-band direct-printing and by the addition of the single word MAY-DEE-CAL pronounced as in French "médical", in radiotelephony.

33.21 § 12 The use of the signals described in No. **33.20** indicates that the message which follows concerns a protected medical transport. The message shall convey the following data:

33.22 *a)* call sign or other recognized means of identification of the medical transport;

33.23 *b)* position of the medical transport;

33.24 *c)* number and type of vehicles in the medical transport;

33.25 *d)* intended route;

33.26 *e)* estimated time en route and of departure and arrival, as appropriate;

33.27 *f)* any other information, such as flight altitude, radio frequencies guarded, languages used and secondary surveillance radar modes and codes.

33.28 § 13 1) The identification and location of medical transports at sea may be conveyed by means of appropriate standard maritime radar transponders (see Recommendation **14 (Mob-87)**).

33.29 2) The identification and location of aircraft medical transports may be conveyed by the use of the secondary surveillance radar (SSR) system specified in Annex 10 to the Convention on International Civil Aviation.

33.30 § 14 The use of radiocommunications for announcing and identifying medical transports is optional; however, if they are used, the provisions of these Regulations and particularly of this Section and of Articles **30** and **31** shall apply.

Section IV – Safety communications

33.31 § 15 In a terrestrial system the announcement of the safety message shall be made on one or more of the distress and safety calling frequencies specified in Section I of Article **31** using digital selective calling techniques. A separate announcement need not be made if the message is to be transmitted through the maritime mobile-satellite service.

33.31A Safety messages transmitted by coast stations in accordance with a predefined timetable should not be announced by digital selective calling techniques. (WRC-03)

33.32 § 16 The safety signal and message shall normally be transmitted on one or more of the distress and safety traffic frequencies specified in Section I of Article **31**, or via the maritime mobile-satellite service or on other frequencies used for this purpose.

33.33 § 17 The safety signal consists of the word SECURITÉ. In radiotelephony, it shall be pronounced as in French.

33.34 § 18 The safety call format or the safety signal indicates that the calling station has an important navigational or meteorological warning to transmit.

33.35 § 19 1) In radiotelephony, the safety message shall be preceded by the safety signal (see No. **33.33**) repeated three times, and the identification of the transmitting station.

33.36 2) In narrow-band direct-printing, the safety message shall be preceded by the safety signal (see No. **33.33**), and the identification of the transmitting station.

33.37 § 20 1) Error correction techniques in accordance with relevant ITU-R Recommendations shall be used for safety messages by direct-printing telegraphy. All messages shall be preceded by at least one carriage return, a line feed signal, a letter shift signal and the safety signal SECURITÉ.

33.38 2) Safety communications by direct-printing telegraphy should normally be established in the broadcast (forward error correction) mode. The ARQ mode may subsequently be used when it is advantageous to do so.

Section V – Transmission of maritime safety information[1]

33.39 *A – General*

33.39A § 20A 1) Messages from ship stations containing information concerning the presence of cyclones shall be transmitted, with the least possible delay, to other mobile stations in the vicinity and to the appropriate authorities at the first point of the coast with which contact can be established. These transmissions shall be preceded by the safety signal.

33.39B 2) Messages from ship stations containing information on the presence of dangerous ice, dangerous wrecks, or any other imminent danger to marine navigation, shall be transmitted as soon as possible to other ships in the vicinity, and to the appropriate authorities at the first point of the coast with which contact can be established. These transmissions shall be preceded by the safety signal.

33.40 § 21 The operational details of the stations transmitting maritime safety information in accordance with Nos. **33.43**, **33.45**, **33.46**, **33.48** and **33.50** shall be indicated in the List of Radiodetermination and Special Service Stations (see also Appendix **13**).

33.41 § 22 The mode and format of the transmissions mentioned in Nos. **33.43**, **33.45**, **33.46** and **33.48** shall be in accordance with the relevant ITU-R Recommendations.

33.42 *B – International NAVTEX system*

33.43 § 23 Maritime safety information shall be transmitted by means of narrow-band direct-printing telegraphy with forward error correction using the frequency 518 kHz in accordance with the international NAVTEX system (see Appendix **15**).

33.44 *C – 490 kHz and 4 209.5 kHz*

33.45 § 24 1) The frequency 490 kHz may be used for the transmission of maritime safety information by means of narrow-band direct-printing telegraphy with forward error correction (see Appendix **15**). (WRC-03)

33.46 2) The frequency 4 209.5 kHz is used exclusively for NAVTEX-type transmission by means of narrow-band direct-printing telegraphy with forward error correction.

33.47 *D – High seas maritime safety information*

33.48 § 25 Maritime safety information is transmitted by means of narrow-band direct-printing telegraphy with forward error correction using the frequencies 4 210 kHz, 6 314 kHz, 8 416.5 kHz, 12 579 kHz, 16 806.5 kHz, 19 680.5 kHz, 22 376 kHz and 26 100.5 kHz.

33.49 *E – Maritime safety information via satellite*

33.50 § 26 Maritime safety information may be transmitted via satellite in the maritime mobile-satellite service using the band 1 530-1 545 MHz (see Appendix **15**).

---

[1] **33.V.1** Maritime safety information includes navigation and meteorological warnings, meteorological forecasts and other urgent messages pertaining to safety normally transmitted to or from ships, between ships and between ship and coast stations or coast earth stations.

Section VI – Intership navigation safety communications

33.51 § 27 1) Intership navigation safety communications are those VHF radiotelephone communications conducted between ships for the purpose of contributing to the safe movement of ships.

33.52 2) The frequency 156.650 MHz is used for intership navigation safety communications (see also Appendix **15** and note *k)* in Appendix **18**).

Section VII – Use of other frequencies for distress and safety

33.53 § 28 Radiocommunications for distress and safety purposes may be conducted on any appropriate communications frequency, including those used for public correspondence. In the maritime mobile-satellite service, frequencies in the bands 1 530-1 544 MHz and 1 626.5-1 645.5 MHz are used for this function as well as for distress alerting purposes (see No. **32.2**).

Section VIII – Medical advice

33.54 § 29 1) Mobile stations requiring medical advice may obtain it through any of the land stations shown in the List of Radiodetermination and Special Service Stations.

33.55 2) Communications concerning medical advice may be preceded by the urgency signal.

ARTICLE 34

Alerting signals in the global maritime distress and safety system (GMDSS)

Section I – Emergency position-indicating radiobeacon (EPIRB) and satellite EPIRB signals

34.1 § 1 The emergency position-indicating radiobeacon signal transmitted on 156.525 MHz and satellite EPIRB signals in the band 406-406.1 MHz or 1 645.5-1 646.5 MHz shall be in accordance with relevant ITU-R Recommendations (see Resolution **27 (Rev.WRC-03)**).

Section II – Digital selective calling

34.2 § 2 The characteristics of the "distress call" (see No. **32.9**) in the digital selective calling system shall be in accordance with relevant ITU-R Recommendations (see Resolution **27 (Rev.WRC-03)**).

RESOLUTION 646 (WRC-03)

Public protection and disaster relief

The World Radiocommunication Conference (Geneva, 2003),

considering

a) that the term “public protection radiocommunication” refers to radiocommunications used by responsible agencies and organizations dealing with maintenance of law and order, protection of life and property and emergency situations;

b) that the term “disaster relief radiocommunication” refers to radiocommunications used by agencies and organizations dealing with a serious disruption of the functioning of society, posing a significant widespread threat to human life, health, property or the environment, whether caused by accident, natural phenomena or human activity, and whether developing suddenly or as a result of complex, long-term processes;

c) the growing telecommunication and radiocommunication needs of public protection agencies and organizations, including those dealing with emergency situations and disaster relief, that are vital to the maintenance of law and order, protection of life and property, disaster relief and emergency response;

d) that many administrations wish to promote interoperability and interworking between systems used for public protection and disaster relief, both nationally and for cross-border operations in emergency situations and for disaster relief;

e) that current public protection and disaster relief applications are mostly narrow-band supporting voice and low data-rate applications, typically in channel bandwidths of 25 kHz or less;

f) that, although there will continue to be narrow-band requirements, many future applications will be wideband (indicative data rates in the order of 384-500 kbit/s) and/or broadband (indicative data rates in the order of 1-100 Mbit/s) with channel bandwidths dependent on the use of spectrally efficient technologies;

g) that new technologies for wideband and broadband public protection and disaster relief applications are being developed in various standards organizations[1];

h) that continuing development of new technologies such as IMT-2000 and systems beyond IMT-2000 and Intelligent Transportation Systems (ITS) may be able to support or supplement advanced public protection and disaster relief applications;

---

1 For example, a joint standardization programme between the European Telecommunications Standards Institute (ETSI) and the Telecommunications Industry Association (TIA), known as Project MESA (Mobility for Emergency and Safety Applications) has commenced for broadband public protection and disaster relief. Also, the Working Group on Emergency Telecommunications (WGET), convened by the United Nations Office for Humanitarian Affairs (OCHA), is an open forum to facilitate the use of telecommunications in the service of humanitarian assistance comprising United Nations entities, major non-governmental organizations, the International Committee of the Red Cross (ICRC), ITU and experts from the private sector and academia. Another platform for coordination and to foster harmonized global Telecommunication for Disaster Relief (TDR) standards is the TDR Partnership Coordination Panel, which has just been established under the coordination of ITU with participation of international telecommunication service providers, related government departments, standards development organizations, and disaster relief organizations.

i) that some commercial terrestrial and satellite systems are complementing the dedicated systems in support of public protection and disaster relief, that the use of commercial solutions will be in response to technology development and market demands and that this may affect the spectrum required for those applications and for commercial networks;

j) that Resolution 36 (Rev. Marrakesh, 2002) of the Plenipotentiary Conference urges Member States to facilitate use of telecommunications for the safety and security of the personnel of humanitarian organizations;

k) that Recommendation ITU-R M.1637 offers guidance to facilitate the global circulation of radiocommunication equipment in emergency and disaster relief situations;

l) that some administrations may have different operational needs and spectrum requirements for public protection and disaster relief applications depending on the circumstances;

m) that the Tampere Convention on the Provision of Telecommunications Resources for Disaster Mitigation and Relief Operations (Tampere, 1998), an international treaty deposited with the United Nations Secretary-General and related United Nations General Assembly Resolutions and Reports are also relevant in this regard,

recognizing

a) the benefits of spectrum harmonization such as:

– increased potential for interoperability;
– a broader manufacturing base and increased volume of equipment resulting in economies of scale and expanded equipment availability;
– improved spectrum management and planning; and
– enhanced cross-border coordination and circulation of equipment;

b) that the organizational distinction between public protection activities and disaster relief activities are matters for administrations to determine at the national level;

c) that national spectrum planning for public protection and disaster relief needs to have regard to cooperation and bilateral consultation with other concerned administrations, which should be facilitated by greater levels of spectrum harmonization;

d) the benefits of cooperation between countries for the provision of effective and appropriate humanitarian assistance in case of disasters, particularly in view of the special operational requirements of such activities involving multinational response;

e) the needs of countries, particularly the developing countries[2], for low-cost communication equipment;

f) that the trend is to increase the use of technologies based on Internet Protocols;

---

2 Taking into account, for example, the ITU-D Handbook on disaster relief.

g) that currently some bands or parts thereof have been designated for existing public protection and disaster relief operations, as documented in Report ITU-R M.2033 [3];

h) that for solving future bandwidth requirements, there are several emerging technology developments such as software-defined radio, advanced compression and networking techniques that may reduce the amount of new spectrum required to support some public protection and disaster relief applications;

i) that in times of disasters, if most terrestrial-based networks are destroyed or impaired, amateur, satellite and other non-ground-based networks may be available to provide communication services to assist in public protection and disaster relief efforts;

j) that the amount of spectrum needed for public protection on a daily basis can differ significantly between countries, that certain amounts of spectrum are already in use in various countries for narrow-band applications, and that in response to a disaster, access to additional spectrum on a temporary basis may be required;

k) that in order to achieve spectrum harmonization, a solution based on regional frequency ranges[4] may enable administrations to benefit from harmonization while continuing to meet national planning requirements;

l) that not all frequencies within an identified common frequency range will be available within each country;

m) that the identification of a common frequency range within which equipment could operate may ease the interoperability and/or inter-working, with mutual cooperation and consultation, especially in national, regional and cross-border emergency situations and disaster relief activities;

n) that when a disaster occurs, the public protection and disaster relief agencies are usually the first on the scene using their day-to-day communication systems, but that in most cases other agencies and organizations may also be involved in disaster relief operations,

noting

a) that many administrations use frequency bands below 1 GHz for narrow-band public protection and disaster relief applications;

b) that applications requiring large coverage areas and providing good signal availability would generally be accommodated in lower frequency bands and that applications requiring wider bandwidths would generally be accommodated in progressively higher bands;

c) that public protection and disaster relief agencies and organizations have an initial set of requirements, including but not limited to interoperability, secure and reliable communications, sufficient capacity to respond to emergencies, priority access in the use of non-dedicated systems, fast response times, ability to handle multiple group calls and the ability to cover large areas as described in Report ITU-R M.2033;

---

[3] 3-30, 68-88, 138-144, 148-174, 380-400 MHz (including CEPT designation of 380-385/390-395 MHz), 400-430, 440-470, 764-776, 794-806 and 806-869 MHz (including CITEL designation of 821-824/866-869 MHz).

[4] In the context of this Resolution, the term “frequency range” means a range of frequencies over which a radio equipment is envisaged to be capable of operating but limited to specific frequency band(s) according to national conditions and requirements.

d) that, while harmonization may be one method of realizing the desired benefits, in some countries, the use of multiple frequency bands can contribute to meeting the communication needs in disaster situations;

e) that many administrations have made significant investments in public protection and disaster relief systems;

f) that flexibility must be afforded to disaster relief agencies and organizations to use current and future radiocommunications, so as to facilitate their humanitarian operations,

emphasizing

a) that the frequency bands identified in this Resolution are allocated to a variety of services in accordance with the relevant provisions of the Radio Regulations and are currently used intensively by the fixed, mobile, mobile satellite and broadcasting services;

b) that flexibility must be afforded to administrations:

– to determine, at national level, how much spectrum to make available for public protection and disaster relief from the bands identified in this Resolution in order to meet their particular national requirements;

– to have the ability for bands identified in this Resolution to be used by all services having allocations within those bands according to the provisions of the Radio Regulations, taking into account the existing applications and their evolution;

– to determine the need and timing of availability as well as the conditions of usage of the bands identified in this Resolution for public protection and disaster relief in order to meet specific national situations,

resolves

1 to strongly recommend administrations to use regionally harmonized bands for public protection and disaster relief to the maximum extent possible, taking into account the national and regional requirements and also having regard to any needed consultation and cooperation with other concerned countries;

2 to encourage administrations, for the purposes of achieving regionally harmonized frequency bands/ranges for advanced public protection and disaster relief solutions, to consider the following identified frequency bands/ranges or parts thereof when undertaking their national planning:

– in Region 1: 380-470 MHz as the frequency range within which the band 380-385/390-395 MHz is a preferred core harmonized band for permanent public protection activities within certain countries of Region 1 which have given their agreement;

– in Region 2[5]: 746-806 MHz, 806-869 MHz, 4 940-4 990 MHz;

– in Region 3[6]: 406.1-430 MHz, 440-470 MHz, 806-824/851-869 MHz, 4 940-4 990 MHz and 5 850-5 925 MHz;

---

5 Venezuela has identified the band 380-400 MHz for public protection and disaster relief applications.

6 Some countries in Region 3 have also identified the bands 380-400 MHz and 746-806 MHz for public protection and disaster relief applications.

3 that the identification of the above frequency bands/ranges for public protection and disaster relief does not preclude the use of these bands/frequencies by any application within the services to which these bands/frequencies are allocated and does not preclude the use of nor establish priority over any other frequencies for public protection and disaster relief in accordance with the Radio Regulations;

4 to encourage administrations, in emergency and disaster relief situations, to satisfy temporary needs for frequencies in addition to what may be normally provided for in agreements with the concerned administrations;

5 that administrations encourage public protection and disaster relief agencies and organizations to utilize both existing and new technologies and solutions (satellite and terrestrial), to the extent practicable, to satisfy interoperability requirements and to further the goals of public protection and disaster relief;

6 that administrations may encourage agencies and organizations to use advanced wireless solutions taking into account *considering h)* and *i)* for providing complementary support to public protection and disaster relief;

7 to encourage administrations to facilitate cross-border circulation of radiocommunication equipment intended for use in emergency and disaster relief situations through mutual cooperation and consultation without hindering national legislation;

8 that administrations encourage public protection and disaster relief agencies and organizations to utilize relevant ITU-R Recommendations in planning spectrum use and implementing technology and systems supporting public protection and disaster relief;

9 to encourage administrations to continue to work closely with their public protection and disaster relief community to further refine the operational requirements for public protection and disaster relief activities;

10 that manufacturers should be encouraged to take this Resolution into account in future equipment designs, including the need for administrations to operate within different parts of the identified bands,

invites ITU-R

1 to continue its technical studies and to make recommendations concerning technical and operational implementation, as necessary, for advanced solutions to meet the needs of public protection and disaster relief radiocommunication applications, taking into account the capabilities, evolution and any resulting transition requirements of the existing systems, particularly those of many developing countries, for national and international operations;

2 to conduct further appropriate technical studies in support of possible additional identification of other frequency ranges to meet the particular needs of certain countries in Region 1 which have given their agreement, especially in order to meet the radiocommunication needs of public protection and disaster relief agencies.

Section II – ITU-R Recommendations and Reports

RECOMMENDATION ITU-R M.693[*,**]

Technical characteristics of VHF emergency position-indicating radio beacons using digital selective calling (DSC VHF EPIRB)

(1990)

The ITU Radiocommunication Assembly,

considering

a) that the alerting and locating functions are parts of the basic requirements of the GMDSS;

b) that chapter IV of the 1988 Amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, permits the carriage of a DSC VHF EPIRB in sea area A1[***] in lieu of a satellite EPIRB;

c) that the characteristics of the digital selective calling system are given in Recommendation ITU-R M.493;

d) that the characteristics of a search and rescue radar transponder (SART) for locating purposes are given in Recommendation ITU-R M.628,

recommends

that the technical characteristics of DSC VHF EPIRBs should be in accordance with Annex I to this Recommendation and with Recommendation ITU-R M.493.

Annex 1

Minimum technical characteristics of DSC VHF EPIRBs

1 General

– DSC VHF EPIRBs should be capable of transmitting distress alerts by digital selective calling and of providing a locating or homing facility. To meet the locating requirements of the GMDSS, Regulation IV/8.3.1 of the 1974 SOLAS Convention requires that a SART (see Recommendation ITU-R M.628) be used for this function.

– The EPIRB should be provided with a battery of sufficient capacity to enable it to operate for a period of at least 48 hours.

---

[*] The Director of the ITU-R is requested to bring this Recommendation to the attention of the International Maritime Organization (IMO).

[**] *Note by the Secretariat* – This Recommendation was amended editorially in March 2006.

[***] "Sea area A1" means an area within the radiotelephone coverage of at least one VHF coast station in which continuous DSC alerting is available, as may be defined by a contracting government to the 1974 SOLAS Convention.

- The EPIRB should be designed to operate under the following environmental conditions:
  - ambient temperatures of –20 °C to +55 °C,
  - icing,
  - relative wind speeds up to 100 knots,
  - after stowage at temperatures between –30 °C and +65 °C.

2 Alerting transmissions

- The alerting signals should be transmitted on the frequency 156.525 MHz using G2B class of emission.
- The frequency tolerance should not exceed 10 parts per million.
- The necessary bandwidth should be less than 16 kHz.
- The emission should be vertically polarized. The antenna should be omnidirectional in the azimuthal plane and sufficiently high to ensure reception of the transmission at the maximum range of the A1 sea area.
- The output power should be at least 100 mW****.

3 DSC message format and transmission sequence

- The technical characteristics for the DSC message should be in accordance with the sequence for the "distress call" specified in Recommendation ITU-R M.493.
- The "nature of distress" indication should be "EPIRB emission" (symbol No. 112).
- The "distress coordinates" and "time" information need not be included. In this case the digit 9 repeated 10 times and the digit 8 repeated four times should be included, respectively, as specified in Recommendation ITU-R M.493.
- The "type of subsequent communication" indication should be "no information" (symbol No. 126) which indicates that no subsequent communications will follow.
- The alerting signals should be transmitted in bursts. Each burst should consist of five successive DSC sequences with the $(N + 1)$th burst of transmission being made with an interval T_n after the (N)th burst as given in Fig. 1, where:

$$T_n = (240 + 10\,N) \text{ s } (\pm 5\%) \text{ and}$$

$$N = 0, 1, 2, 3, \ldots, \text{etc.}$$

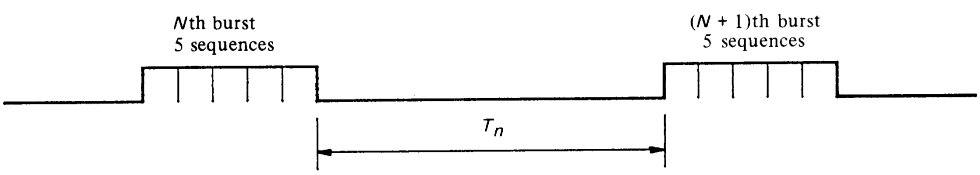


FIGURE 1

D01-sc

**** The output power required to carry a ship-to-shore alert at the maximum range of the A1 sea area should be at least 6 W with an appropriate antenna height above sea level.

RECOMMENDATION ITU-R M.830-1*

Operational procedures for mobile-satellite networks or systems in the bands 1 530-1 544 MHz and 1 626.5-1 645.5 MHz which are used for distress and safety purposes as specified for the GMDSS

(Question ITU-R 90/8)

(1992-2005)

Scope

This Recommendation provides operational procedures for mobile-satellite networks or systems in the bands 1 530-1 544 MHz and 1 626.5-1 645.5 MHz which are used for distress and safety purposes as specified for the GMDSS. The means to ensure the necessary priority access for maritime mobile-satellite distress and safety communications are given in the Recommendation.

The ITU Radiocommunication Assembly,

considering

a) that multiple mobile-satellite networks or systems are operating or being developed to operate in the 1 530-1 544 MHz and 1 626.5-1 645.5 MHz bands;

b) that the bands 1 530-1 544 MHz and 1 626.5-1 645.5 MHz (Radio Regulations (RR) Appendix 15, Table 15-2) available for GMDSS distress and safety communications are also available for other radio services;

c) that with the introduction of mobile-satellite networks or systems within these frequency bands, some of which may not be participants in the GMDSS, the integrity, effectiveness and protection of distress and safety communications must be continuously maintained;

d) that maritime mobile-satellite distress and safety communications must be protected from harmful interference (see RR No. 5.353A);

e) that maritime distress and safety communications require priority access with real time preemptive capability or dedicated channels in the mobile-satellite service;

f) that account must be taken of the priority of safety-related communications (Article 53 of the RR);

g) that maritime mobile-satellite distress and safety communications must be relayed to the appropriate Rescue Coordination Centres (RCCs) in the most rapid and expedient manner;

h) that priority relay of distress alerts from ships in distress to the appropriate RCCs must be preserved and be in accordance with Article 53 of the RR;

j) that internetwork or intersystem linking of mobile-satellite systems may be provided via means other than the mobile-satellite service links operating in the 1.5-1.6 GHz frequency bands,

---

* This Recommendation should be brought to the attention of the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO) and ITU-T.

recommends

1 that mobile-satellite networks or systems participating in the GMDSS should be equipped with the means for intersystem linking between coast earth stations;

2 that mobile-satellite networks or systems operating in the frequency bands 1 530-1 544 MHz and 1 626.5-1 645.5 MHz participating in the GMDSS should be equipped with the means to ensure that maritime mobile-satellite distress and safety communications are given the necessary priority access with real time preemptive capability or dedicated channels to ensure the most expeditious handling and relay of the messages to the appropriate RCCs;

NOTE 1 – Section 2 does not apply to MSS systems providing distress and safety services, for which the technical and operational characteristics have already been established in accordance with the relevant provisions of the RR or of the IMO, as applicable.

3 that communications of mobile-satellite system stations operating in the frequency bands 1 530-1 544 MHz and 1 626.5-1 645.5 MHz not participating in the GMDSS shall operate on a secondary basis to distress and safety communications of stations operating in the GMDSS. Account shall be taken of the priority of safety-related communications in the other mobile-satellite services.

RECOMMENDATION ITU-R S.1001-1*

Use of systems in the fixed-satellite service in the event of natural disasters and similar emergencies for warning and relief operations

(1993-2006)

Scope

This Recommendation provides guidelines on the use of satellite networks in the event of natural disasters and similar emergencies. This Recommendation provides information about the overall system and terminal design which is suitable for disaster relief telecommunication.

This Recommendation responds to the requirements of the Tampere Convention (2005).

The ITU Radiocommunication Assembly,

considering

a) that reliable and rapid deployment of telecommunication equipment is essential for relief operations in the event of natural disasters and similar emergencies;

b) that inherent to natural disaster events is the unpredictability of the site location thus implying the need for prompt on-site transportation of the telecommunication equipment;

c) that satellite transmission using small aperture earth stations, such as fixed VSATs, vehicle-mounted earth stations and transportable earth stations is invaluable and at times is one of the most viable solutions to provide emergency telecommunication services for relief operations;

d) that the telecommunication equipment might perform a variety of functions including, but not limited to, voice telecommunication, field reporting, data collection and video transmission;

e) that it would be useful to provide technical parameters of small aperture earth stations and give examples of systems for emergency purposes as guidelines to plan the use of systems for warning and relief operations,

recommends

1 that when planning the use of systems in the fixed-satellite service for warning and relief operations in the event of natural disasters and similar emergencies, the material in Annex 1 should be taken into consideration;

2 that the following Notes should be regarded as part of this Recommendation:

NOTE 1 – The logistics of the transportation, installation and operation of the telecommunication equipment requires careful consideration in order to maximize the system performance in terms of reliability and deployment rapidity.

NOTE 2 – Although the use of transportable earth stations for disaster management makes it impractical to undertake detailed prior coordination and interference assessment, attention should be paid to these aspects when using shared frequency bands.

* See Recommendation ITU-R SNG.1421 for information on using small earth stations for the transmission of television signals.

Annex 1

The use of small earth stations for relief operation in the event of natural disasters and similar emergencies

1 Introduction

In the event of natural disasters, epidemics and famines, etc., there is an urgent need for a reliable communication link for use in relief operations. Satellite appears as the most appropriate means to quickly set up a communication link with remote facilities. The main requirements of such a satellite system are discussed here. Assuming the system is to operate in the fixed-satellite service (FSS), it is desirable that a small earth station, such as a fixed VSAT, a vehicle-mounted earth station or a transportable earth station, with access to an existing satellite system, should be available for transportation to, and installation at, the disaster area. It is also desirable that the system relies on widespread standards so that:

– equipment is readily available;
– interoperability is ensured;
– reliability is ensured.

This Annex provides material that may be useful in planning the use of systems in the FSS in the event of natural disasters and similar emergencies for warning and relief operations.

2 Basic considerations

2.1 Required services

The basic communication architecture for relief operations should be composed of a link connecting the disaster area with designated relief centres, and its basic telecommunication services should comprise at least telephony, any kind of data (IP, datagrams, facsimile, ...), video. For such transmission, digital transmission technologies are employed in most cases.

2.2 Channel and physical layer requirements

In digital transmissions, one means to measure the performance of the coded channel is the bit error probability (BEP). The recommended objective BEP in the FSS provided in Recommendation ITU-R S.1062 is 10^{-6} for 99.8% of time in the worst month. This BEP results both from the SNIR (signal-to-noise and interference ratio), which is the performance of the channel, and from the coding. Appropriate coding can compensate, to a certain extent, for poor channel quality but lowers the useful bit rate.

The particular conditions of transmission in the place of a disaster in case of both warning and relief operation (e.g. climate of site, nature of mission, …), which might degrade the channel quality, should be taken into account by reinforcing coding. The ideal would be to have adaptive coding, i.e. a system able to get back information from the channel and to respond by adapting the coding rate.

2.3 Network requirements

For relief operations, due to the essential requirement of having small antennas, it is preferable to operate the network in the 14/12 GHz band or even in the 30/20 GHz band. Although the bands such as 6/4 GHz require larger antennas, they are also suitable depending on conditions of transmission and coverage of satellite resources. In order to avoid interference, it should be taken into account that some bands are shared with terrestrial services.

The network should offer suitable quality of service. In case the network is shared with customers having non-urgent needs, the emergency operations should have absolute priority which means a "pre-emption" class of service. A fully private network, with reserved frequency bands and facilities, could be desirable.

When the number of operational earth stations is large, a network control based on demand assignment multiple access (DAMA) may be necessary.

2.4 Associated earth station

For (a) small earth station(s) on site, a vehicle-mounted earth station or a transportable earth station should be considered. The material provided in § 3 to 6 of this Annex may be useful for sizing of such earth stations.

For the smooth operation of earth stations in the event of a disaster, regular training for potential operators and preparatory maintenance of the equipment is essential. Particularly, special attention should be given to the inclusion of autonomous battery or power systems.

3 Required earth station e.i.r.p. levels and satellite resources

In this section, required earth station e.i.r.p. levels and satellite resources are studied by link budget calculations based on the assumption that a small earth station (a fixed VSAT, a vehicle-mounted earth station or a transportable earth station) operating in the disaster area communicates with a hub earth station equipped with a larger antenna.

The choice of system parameters should be based on considerations listed in this section of this Annex for the 6/4 GHz band, the 14/12 GHz and the 30/20 GHz band. The system parameters are listed in Table 1a) to 1f).

TABLE 1

Typical satellite, earth station, carrier parameter for calculation

a) *Distance to GSO satellite and path loss*

Elevation (degrees)	10
Distance (km)	40 600

b) *Path loss (EL = 10°)*

Frequency (GHz)	**6/4**		**14/12**		**30/20**	
	4.0	6.2	12.25	14.25	20.0	30.0
Wavelength (m)	0.08	0.05	0.02	0.02	0.02	0.01
Path loss (dB)	196.7	200.5	206.4	207.7	210.6	214.2

c) *Transmission channel parameter*

Modulation FEC	QPSK 1/2 Conv.(1)	QPSK 3/4 Conv.(1)	QPSK 1/2 Conv.(1)	QPSK 1/2 turbo coding	8-PSK 2/3
BER	10^{-6}	10^{-6}	10^{-6}	10^{-6}	10^{-6}
Required E_b/N_0 (dB)	6.1	7.6	4.4	3.1	9.0
FEC rate	0.5	0.75	0.5	0.5	0.67
Outer code rate	1.0	1.0	188/204	1.0	1.0
Number of bits in a symbol	2	2	2	2	3
Required C/N (dB)	6.1	9.4	4.0	3.1	12.0

(1) Constraint length $k = 7$.

d) *Earth station antenna gain and G/T*

Frequency band (GHz)	6/4				14/12				30/20			
Antenna diameter	2.5 m		5.0 m		1.2 m		3.0 m		1.2 m		2.4 m	
Frequency (GHz)	4.0	6.2	4.0	6.2	12.25	14.25	12.25	14.25	20.0	30.0	20.0	30.0
Efficiency	0.6	0.6	0.6	0.6	0.6	0.6	0.6	0.6	0.6	0.6	0.6	0.6
Antenna gain (dBi) peak	38.2	42.0	44.2	48.0	41.5	42.8	49.5	50.8	45.8	49.3	51.8	55.3
G/T (dB/K)	17.5		23.5		20.8		28.8		25.1		31.1	

e) *HUB earth station antenna gain and G/T*

Frequency (GHz)	6/4		14/12		30/20	
	4.0	6.2	12.25	14.25	20.0	30.0
Antenna gain (dBi)	55.7	59.5	57.9	59.5	58.0	61.8
HUB earth station G/T (dB/K)	35.0		35.0		35.0	
HUB earth station antenna size (m)	18 m		7.6 m		4.7 m	

f) *The satellite transponder gain*

Satellite	6/4 GHz satellite	14/12 GHz satellite	30/20 GHz satellite
Frequency band (GHz)	6/4	14/12	30/20
Wavelength (m)	0.05	0.02	0.01
Beam type	GLOBAL	SPOT	Multi
Satellite receive G/T (dB/K)	−13.0	2.5	11.0
Transponder saturation e.i.r.p. for single carrier (dBW)	29.0	45.8	54.5
SFD (dB(W/m^2))	−78.0	−83.0	−98.4
IBO-OBO (dB)	1.8	0.9	5.0
Gs (dB)	37.3	44.5	51.0
Transponder gain #a (dB)	146.1	174.2	200.2
Transponder gain #b (dB)	−55.3	−33.5	−14.0

SFD: Saturation flux-density

IBO: Input back-off

OBO: Output back-off

QPSK with rate 1/2 convolutional code, 3/4 convolutional code, 1/2 convolutional code + 188/204 Reed Solomon outer code and 1/2 turbo code are typical digital modulation and FEC methods commonly used for FSS satellite links. It is worth stressing that the combination of a convolutional code as the inner code with a Reed-Solomon code as the outer code is now rendered obsolete by turbo coding or low density parity check (LDPC) coding which performs better in general; the former coding scheme is surviving as a past legacy.

The antenna diameter of a small earth station (vehicle-mounted or transportable) is assumed to be 2.5 m or 5 m for the 6/4 GHz band and 1.2 m or 3 m for the 14/12 GHz band and 1.2 m or 2.4 m for the 30/20 GHz band in this example of the link budget calculation. For 14/12 GHz and 30/20 GHz stations, smaller diameter antennas may be used if appropriate measures, such as satellites with greater *G*/*T* or spread spectrum techniques are used to allow reduction of the off-axis emissions to acceptable levels.

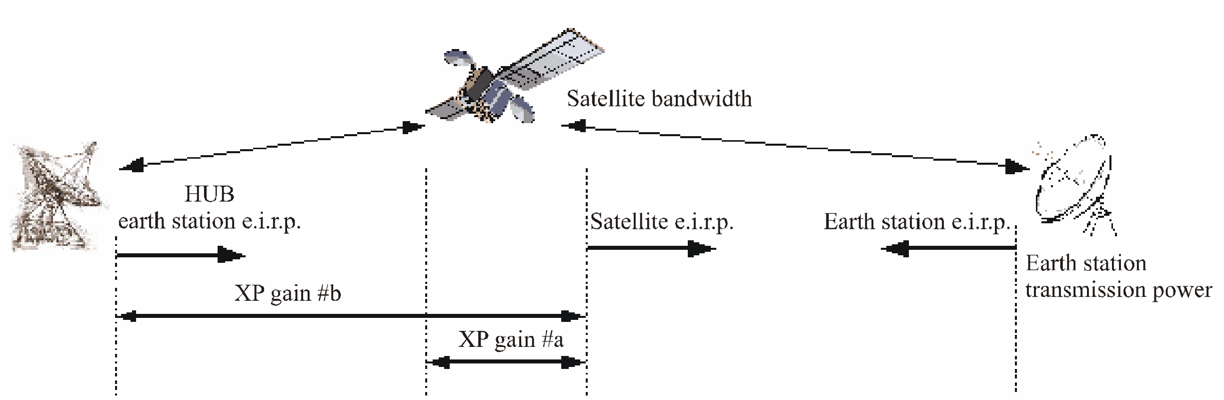
In the 4 GHz band, a typical *G*/*T* of an earth station is 17.5 dB/K and 23.5 dB/K for the 2.5 m and 5 m antenna, respectively. In the 12 GHz band, a typical *G*/*T* of an earth station is 20.8 dB/K and 28.8 dB/K for the 1.2 m and 3 m antenna, respectively. In the 20 GHz band, a typical *G*/*T* of an earth station is 25.1 dB/K and 31.1 dB/K for the 1.2 m and 2.4 m antenna, respectively. The noise temperature of low noise amplifier is assumed to be 60 K, 100 K and 140 K for the 4 GHz band, the 12 GHz band and the 20 GHz band, respectively. Although small aperture antennas such as 45, 75 cm, etc. can be used, Radio Regulations including the off-axis limitation should be considered when using those antennas. The use of small antennas may not allow meeting the off-axis emission criteria, therefore, the earth station transmit power should be reduced in order to avoid the interference to adjacent satellites and other services.

It should be noted that values of satellite e.i.r.p. and earth station e.i.r.p. are for a small earth station with antenna elevation 10° and 2 dB of the total margin.

In Table 1f), typical satellite parameters for global beams in the 6/4 GHz band, spot beams in the 14/12 GHz band and the 30/20 GHz band are provided. The "transponder gain #a" and "transponder gain #b" in Table 1f), are defined as shown in Fig. 1.

FIGURE 1

Definition of transponder gain (XP gain)



XP gain #a = *Gs* + e.i.r.p. (satellite saturation) SFD + Δ (IBO-OBO)
XP gain #b = satellite e.i.r.p. HUB earth station e.i.r.p.
Gs: Antenna gain of 1 m^2

1001-01

As a result of link budget calculation of the outbound (hub-to-VSAT) and inbound (VSAT-to-hub) direction, Tables 2a), 2b) and 2c) provide examples of required earth station e.i.r.p. levels and satellite resources including the required satellite e.i.r.p., the earth station e.i.r.p. and the bandwidth required for typical digital modulation and FEC methods in the 6/4 GHz band, the 14/12 GHz and the 30/20 GHz band.

TABLE 2a

Examples of the required earth station e.i.r.p. levels and satellite resources in 6/4 GHz band

IR(1)	Modulation/FEC	QPSK 1/2 Conv.(2)		QPSK 3/4 Conv.(2))		QPSK 1/2 Conv.(2) + RS		QPSK 1/2 TC	
	Antenna diameter	**2.5 m**	**5.0 m**	**2.5 m**	**5.0 m**	**2.5 m**	**5.0 m**	**2.5 m**	**5.0 m**
64 kbit/s	Allocated satellite bandwidth (kHz)	90	90	60	60	90	90	60	60
	Satellite e.i.r.p. (dBW)	6.8	0.9	8.3	2.4	6.8	0.9	8.3	2.4
	Earth station e.i.r.p. (dBW)	46.2	46.2	47.7	47.7	46.2	46.2	47.7	47.7
	Earth station transmit power (W)	3.1	0.8	4.4	1.1	3.1	0.8	4.4	1.1
1 Mbit/s	Allocated satellite bandwidth (kHz)	1 434	1 434	956	956	1 434	1 434	956	956
	Satellite e.i.r.p. (dBW)	18.8	12.9	20.3	14.4	18.8	12.9	20.3	14.4
	Earth station e.i.r.p. (dBW)	58.2	58.2	59.7	59.7	58.2	58.2	59.7	59.7
	Earth station transmit power (W)	50.3	12.6	71.1	17.8	50.3	12.6	71.1	17.8
6 Mbit/s	Allocated satellite bandwidth (kHz)	8 602	8 602	5 734	5 734	8 602	8 602	5 734	5 734
	Satellite e.i.r.p. (dBW)	26.6	20.7	28.1	22.2	26.6	20.7	28.1	22.2
	Earth station e.i.r.p. (dBW)	66.0	66.0	67.5	67.5	66.0	66.0	67.5	67.5
	Earth station transmit power (W)	302.1	75.5	426.7	106.7	302.1	75.5	426.7	106.7

(1) IR: Information rate.

(2) Constraint length $K = 7$.

TABLE 2b

Examples of the required earth station e.i.r.p. levels and satellite resources in 14/12 GHz band

IR(1)	Modulation/FEC	QPSK 1/2 Conv.(2)		QPSK 3/4 Conv.(2)		QPSK 1/2 Conv.(2) + RS		QPSK 1/2 TC	
	Antenna diameter	**1.2 m**	**3.0 m**	**1.2 m**	**3.0 m**	**1.2 m**	**3.0 m**	**1.2 m**	**3.0 m**
64 kbit/s	Allocated satellite bandwidth (kHz)	90	90	60	60	97	97	90	90
	Satellite e.i.r.p. (dBW)	14.7	7.4	16.2	8.9	13.0	5.7	11.7	4.4
	Earth station e.i.r.p. (dBW)	35.6	35.6	37.1	37.1	33.9	33.9	32.6	32.6
	Earth station transmit power (W)	0.3	0.1	0.5	0.1	0.2	0.04	0.2	0.03
1 Mbit/s	Allocated satellite bandwidth (kHz)	1 434	1 434	956	956	1 556	1 556	1 434	1 434
	Satellite e.i.r.p. (dBW)	26.7	19.4	28.2	20.9	25.0	17.7	23.7	16.4
	Earth station e.i.r.p. (dBW)	47.7	47.7	49.2	49.2	46.0	46.0	44.7	44.7
	Earth station transmit power (W)	5.3	0.9	7.5	1.2	3.6	0.6	2.7	0.4
6 Mbit/s	Allocated satellite bandwidth (kHz)	8 602	8 602	5 734	5 734	9 334	9 334	8 602	8 602
	Satellite e.i.r.p. (dBW)	34.5	27.2	36.0	28.7	32.8	25.5	31.5	24.2
	Earth station e.i.r.p. (dBW)	55.4	55.4	56.9	56.9	53.7	53.7	52.4	52.4
	Earth station transmit power (W)	32.0	5.1	45.1	7.2	21.6	3.5	16.0	2.6

(1) IR: Information rate.

(2) Constraint length $K = 7$.

TABLE 2c

Examples of the required earth station e.i.r.p. levels and satellite resources in 30/20 GHz band

IR(1)	Modulation/FEC	QPSK 1/2 Conv.(2)		QPSK 3/4 Conv.(2)		QPSK 1/2 Conv.(2) + RS		QPSK 1/2 TC	
	Antenna diameter	**1.2 m**	**2.4 m**	**1.2 m**	**2.4 m**	**1.2 m**	**2.4 m**	**1.2 m**	**2.4 m**
64 kbit/s	Allocated satellite bandwidth (kHz)	90	90	60	60	97	97	90	90
	Satellite e.i.r.p. (dBW)	25.8	25.5	27.3	27.0	24.1	23.8	22.8	22.5
	Earth station e.i.r.p. (dBW)	30.7	30.7	32.2	32.2	29.0	29.0	27.7	27.7
	Earth station transmit power (W)	0.024	0.006	0.035	0.009	0.017	0.004	0.012	0.003
1 Mbit/s	Allocated satellite bandwidth (kHz)	1 434	1 434	956	956	1 556	1 556	1 434	1 434
	Satellite e.i.r.p. (dBW)	37.9	37.6	39.4	39.1	36.2	35.9	34.9	34.6
	Earth station e.i.r.p. (dBW)	42.8	42.8	44.3	44.3	41.1	41.1	39.8	39.8
	Earth station transmit power (W)	0.4	0.1	0.6	0.1	0.3	0.1	0.2	0.05
6 Mbit/s	Allocated satellite bandwidth (kHz)	8 602	8 602	5 734	5 734	9 334	9 334	8 602	8 602
	Satellite e.i.r.p. (dBW)	45.6	45.4	47.1	46.9	43.9	43.7	42.6	42.4
	Earth station e.i.r.p. (dBW)	50.6	50.6	52.1	52.1	48.9	48.9	47.6	47.6
	Earth station transmit power (W)	2.3	0.6	3.3	0.8	1.6	0.4	1.2	0.3

(1) IR: Information rate.

(2) Constraint length $K = 7$.

As the required bandwidth shows for one direction, twice the listed value is needed for both directions. The required satellite e.i.r.p. shows the one for the downlink of outbound direction which is usually under a power limited situation at satellites. The required earth station e.i.r.p. and transmit power shows the one for the uplink of inbound direction which is usually under a power limited situation at earth stations.

Rain attenuation is not included in the above calculations. Depending on local conditions, provision for rain margin may be needed. The interference or intermodulation is not taken into account. Therefore, additional margin is needed. (See Recommendation ITU-R P.618 for the rain attenuation for local climate and Recommendation ITU-R S.1432 for the various interference criteria.)

3.1 Example of link budget calculation

For illustrative purpose, details of the link budget calculation of Table 2a (in case of 6 Mbit/s of 6/4 GHz band with QPSK 1/2 Conv., 2.5 m antenna) are shown in Table 3a.

A mark of (2) in Table 3a are the values listed in Table 2a as results of calculation.

4 Configuration of the transportable earth station

The earth station may be divided into the following major subsystems:

- antenna,
- power amplifier,
- low noise receiver,
- ground communication equipment,

– control and monitoring equipment,
– terminal equipment, including facsimile and telephones,
– support facilities.

This Section should be referred to as a guideline of actual characteristics of the system and small earth stations such as transmission capability, weight/size and performance of the subsystem.

4.1 Weight and size

All the equipment, including shelters, should be capable of being packaged into units of weight which can be handled by a few persons. Furthermore, the total volume and weight should not be in excess of that which could be accommodated in the luggage compartment of a passenger jet aircraft. This is readily attainable with present-day technology. The allowable size and weight specifications of the various aircraft should be consulted during the design of satellite terminals for disaster relief telecommunications.

TABLE 3a

The link budget calculation of Table 2a
(6 Mbit/s of C band with QPSK 1/2 Conv., 2.5 m antenna)

Item	Unit	Value
A. Transmission channel parameter		
Modulation		QPSK 1/2 Conv.(1)
BER		10^{-6}
Required E_b/N_0 (dB)	dB	6.1
Required C/N (dB)	dB	6.1
B. Satellite main parameter		
SFD (beam edge)	dB(W/m^2)	−78.0
G/T (beam edge)	dB/K	−13.0
Transponder saturation e.i.r.p. for single carrier (beam edge) (dBW)	dBW	29.0
IBO	dB	−5.4
OBO	dB	−4.5
Δ(IBO-OBO)	dB	0.9
Gain of 1 square metre	dB	37.3
TP gain (#a)	dB	145.2
C. Transmission carrier parameter		
Information rate	kbit/s	6 144.0
FEC rate		0.5
RS (Reed Solomon) rate		1.0
Transmission rate	kbit/s	12 288.0
Noise bandwidth	kHz	6 144.0
Allocated bandwidth(2)	kHz	8 601.6(2)

(1) Constraint length $K = 7$

TABLE 3a (*end*)

D. Earth station main parameter			
G/T	dB/K	17.5 (2.5 m earth station)	35.0 (HUB earth station)
E. Link budget calculation			
		Outbound **(HUB ≥ 2.5 m earth station)**	**Inbound** **(2.5m earth station ≥ HUB)**
1. Uplink C/N (HUB E/S –> satellite			
HUB/earth station e.i.r.p.	dBW	81.9	66.0(2)
Free space loss (6 GHz)	dB	200.5	200.5
Satellite G/T (beam edge)	dB/K	−13.0	−13.0
C/N (a)	dB	29.1	13.21
2. IM (intermodulation) of earth station			
C/N (b)	dB	99.0	99.0
3. IM (intermodulation) of satellite			
C/N (c)	dB	99.0	99.0
4. Downlink C/N (satellite –> E/S)			
Satellite EIRP (beam edge)	dBW	26.6(2)	10.7
Pattern advantage etc.	dB	0.0	0.0
Free space loss (4 GHz)	dB	196.7	196.7
Earth station G/T	dB/K	17.5	35.0
C/N (d)	dB	8.1	9.7
5. Co-channel interference			
C/N (e)	dB	99.0	99.0
Total *C/N* (*C/N* (a) ~ *C/N* (e))	dB	8.1	8.1
Margin	dB	2.0	2.0
Total C/N	dB	6.1	6.1
Transponder gain (#b)	dB	−55.3	
Feed loss	dB		0.8
Antenna gain of earth station (2.5 m)	dBi		42.0
Required earth station transmit power	W		302.1(2)

4.2 Antenna

One of the major requirements for the antenna is ease of erection and transportation. For this purpose, the antenna reflector could consist of several panels made of light material such as fibre reinforced plastic or aluminium alloy. The use of an antenna of a diameter from 2.5 to 5 m is foreseen for use in the 6/4 GHz band. However, for other frequency bands, antenna construction requirements are eased because smaller antenna sizes can be used.

The main antenna reflector may be illuminated by a front-fed horn or a feed which includes a sub-reflector. The latter type may have a slight advantage in G/T performance, since the curvature of both the sub-reflector and main reflector can be optimized, but ease of erection and alignment may take precedence over G/T considerations.

A manual or automatic pointing system may be provided commensurate with weight and power consumption, by monitoring a carrier signal from the satellite, having a steerable range of approximately ±5°.

4.3 Power amplifier

Air-cooled klystron and TWT (helix-type) amplifiers are both suitable for this application, but from the point of view of efficiency and ease of maintenance, the former is preferred.

Although the instantaneous transmission bandwidth is small, the output amplifier may need to have the capability of being tuneable over a wider bandwidth, e.g. 500 MHz, since the available satellite channel may be anywhere within this bandwidth.

For power requirements less than 100 W, a solid state power amplifier (FET) would also be suitable.

In the 30 GHz band, solid-state, TWT and klystron amplifiers are suitable for this application.

4.4 Low-noise receiver

Because the low-noise receiver must be small, light and be capable of easy handling with little maintenance, an uncooled low noise amplifier is the most desirable.

A temperature of 50 K has been realized and even lower temperatures are expected in the future in the 4 GHz band. An FET amplifier is more suitable from the point of view of size, weight and power consumption than a parametric amplifier. A noise temperature of 50 K in the 4 GHz band and 150 K in the 12 GHz band has been realized by FET amplifiers. In the 20 GHz band, an FET amplifier with a noise temperature of 300 K or less at room temperature has been realized.

Appendix 1
to Annex 1

Examples of transportable earth station realizations and system implementation

1 Small transportable earth stations

In the 14/12 GHz and 30/20 GHz bands, most of the transportable stations have antennas with around 1.2 m diameters.

1.1 Examples of air transportable and vehicle equipped small earth stations in the 14/12 GHz band

Various types of small earth station equipment have been developed for the use of new satellite communication systems in the 14/12 GHz band. For implementing small earth stations, efforts have been made to decrease the size and to improve transportability so as to ease their use for general applications. This allows the occasional or temporary use of these earth stations for relief operation elsewhere in the country or even worldwide. Such temporary earth stations are installed either in a vehicle or use portable containers with a small antenna. It is thus possible to use them in an emergency.

The vehicle equipped earth station in which all the necessary equipment is installed in the vehicle, e.g. a four-wheel drive van, permits operation within 10 min of arrival including all necessary actions such as antenna direction adjustments.

A portable earth station is disassembled prior to transportation and reassembled at the site within approximately 15 to 30 min. The size and weight of the equipment generally allow it to be carried by hand by one or two persons, and the containers are within the limit of the IATA checked luggage regulations. Total weight of this type of earth station including power generator and antenna assembly is reported to be as low as 150 kg, but 200 kg is more usual. It is also possible to carry the equipment by helicopters.

Examples of small transportable earth stations for use with Japanese communication satellites in the 14/12 GHz band are shown in Table 4.

1.2 Examples of small transportable earth stations for operation at 30/20 GHz

Several types of 30/20 GHz small transportable earth stations, which can be transported by a truck or a helicopter, have been manufactured and operated satisfactorily in Japan.

Examples of small transportable earth stations for operation at 30/20 GHz are shown in Table 5.

TABLE 4

Example of small transportable earth stations for the 14/12 GHz band

Example No.	1	2	3	4(1)	5	6
Type of transportation	Vehicle equipped					
Antenna diameter (m)	2.6 × 2.4	1.8	1.2	1.8	0.9	1.5 × 1.35
e.i.r.p. (dBW)	72	70	62.5	65.1-71.2 (95-400 W)(2)	54-64 (20-200 W)(2)	72 (400 W)(2)
RF bandwidth (MHz)	24-27	20-30	30	1.4-60 Mbit/s	64 kbit/s-60 Mbit/s	1.4-60 Mbit/s
Total weight	6.4 tons	6.0 tons	2.5 tons	250 kg(3)	70 kg(4)	210 kg
Package: – Total dimensions (m) – Total number – Max. weight (kg)	– – –	– – –	– – –	2.62 × 1.95 × 0.88 – < 345 kg	1.2 × 1.1 × 0.4 1 –	2.37 × 1.53 × 0.45 1 –
Capacity of engine generator or power consumption	7.5 kVA	10 kVA	5 kVA	~ 4 100 W	~ 4 100 W	~ 4 100 W
Required number of persons	1-2	1-2	1-2	1	1	1

TABLE 4 (*end*)

Example No.	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Type of transportation	Air transportable								
Antenna diameter (m)	1.8	1.4	1.2	0.75	0.9	0.9 × 0.66	1	0.9	0.9 × 0.66
e.i.r.p. (dBW)	70	64.9	62.5	42.5	44.0	51.7	55	66	51.7
RF bandwidth (MHz)	20-30	30	30	Up to 0.5	Up to 0.5	2	6	64 k ~ 60 Mbit/s	64 k ~ 4 Mbit/s
Total weight (kg)	275	250	200	131	141	100	110	130	39
Package: – Total dimensions (m) – Total number – Max. weight (kg)	 < 2 10 45	 < 2 13 34	 < 2 8 20	 1 5 37	 1.2 5 37	 – – –	 – – –	 1 × 0.6 × 1.2 3 (5) < 43 kg	 70 × 47 × 31 (cm) 1 39 kg
Capacity of engine generator or power consumption	3 kVA	0.9-1.3 kVA	1.0 kVA	< 370 W	< 370 W	< 2 kVA	< 2 kVA	~ 4 100 W	750 W
Required number of persons	2-3	2-3	1-2	1-2	1-2	2	3	1	1

(1) Flyaway

(2) The amplifier size is selectable for the purpose.

(3) Total weight dose not include the weight of the car.

(4) Without amplifier.

(5) There are three packages: the sizes are 72 × 60 × 26 (cm), 51 × 29 × 40 (cm), and 100 × 60 × 40 (cm) respectively.

TABLE 5

Examples of small transportable earth stations for the 30/20 GHz band

Operating frequency (GHz)	**Total weight (tons)**	**Power requirement (kVA)**	**Antenna**		**Maximum e.i.r.p. (dBW)**	***G/T* (dB/K)**	**Type of modulation**	**Total setting-up time (h)**	**Normal location of earth station**
			Diameter (m)	**Type**					
30/20	5.8	12	2.7	Cassegrain	76	27	FM (colour TV 1 channel) (1) or FDM-FM (132 telephone channels)	1	On a truck
	2	9	3	Cassegrain (2)	79.8	27.9	FM (colour TV 1 channel) (1) and ADPCM-BPSK-SCPC (3 telephone channels)	1	On the ground
	1	1 (3)	2	Cassegrain	56.3	20.4	ADM-QPSK-SCPC (1 telephone channel)	1.5	On the ground
	3.5 (4)	< 8.5	1.4	Offset Cassegrain	68	20	Digital-TV (3 voice channels are multiplexed) (1) or 1 voice channel	> 1	On a van/SUV
	0.7	3	1	Cassegrain	59.9	15.2	FM-SCPC (1 telephone channel) or DM-QPSK-SCPC (1 telephone channel)	1	On a truck

(1) One-way.

(2) The reflector is divided into three sections.

(3) Excluding power for air conditioning.

(4) Include vehicle.

2 Example of an emergency network and associated earth stations

2.1 Example of an emergency network in Italy using the 14/12 GHz band

An emergency satellite network has been designed and implemented in Italy for operation in the 14/12.5 GHz frequency band via a EUTELSAT transponder. This dedicated network, which is based on the use of wholly digital techniques, provides emergency voice and data circuits and a time shared compressed video channel for relief operations and environmental data collection. The network architecture is based on a dual sub-networking star configuration, for the two services and makes use of a TDM-BPSK and an FDMA-TDMA-BPSK dynamic transmission scheme, respectively for the outbound and inbound channels. The ground segment is composed of: a master common hub station for the two star networks, which is a fixed-earth station having a 9 m antenna and a 80 W transmitter; a small number of transportable earth stations, having antennas of 2.2 m and 110 W transmitters; a number of fixed data transmission platforms with 1.8 m dishes and 2 W solid state power amplifier transmitters.

These platforms have a receive capability (*G*/*T* of 19 dB/K), in order to be remotely controlled by the master station, and their average transmit throughput is 1.2 kbit/s. The transportable earth stations are mounted on a lorry, but if necessary, can also be loaded in a cargo helicopter for fast transportation. They have a *G*/*T* of 22.5 dB/K and are equipped with two sets of equipment each containing one 16 kbit/s (vocoder) voice channel and one facsimile channel at 2.5 kbit/s. These earth stations which are also able to transmit a compressed video channel at 2.048 Mbit/s in SCPC-BPSK, are remotely controlled by the master station. The major features of this *ad hoc* emergency network are summarized in Table 6.

TABLE 6

Example of an emergency satellite communication network operating at 14/12 GHz

Station designation	**Antenna diameter (m)**	***G/T* (dB/K)**	**Trans-mitter power (W)**	**Primary power requirement (kVA)**	**Transmission scheme**		**Service capability**
Master	9.0	34.0	80	15.0	Tx	512 kbit/s-TDM/BPSK (+ FEC 1/2)	12 × 16 kbit/s (vocoder) voice channels
					Rx	“*n*” × 64 kbit/s-FDMA/TDMA/BPSK (+ FEC 1/2) and 2.048 Mbit/s-SCPC/QPSK (+ FEC 1/2)	12 × 2.4 kbit/s facsimile channels 1 × 2.048 Mbit/s video channel
Peripherals (transportable)	2.2	22.5	110	2.0	Tx	64 kbit/s-TDMA/BPSK (+ FEC 1/2) and 2.048 Mbit/s-SCPC/QPSK (+ FEC 1/2)	2 × 16 kbit/s (vocoder) voice channels 2 × 2.4 kbit/s facsimile channels
					Rx	512 kbit/s-TDM/BPSK (+ FEC 1/2)	1 × 2.048 Mbit/s video channel
Unattended platforms	1.8	19.0	2	0.15	Tx	64 kbit/s-TDMA/BPSK (+ FEC 1/2)	1 × 1.2 kbit/s data transmission channel
					Rx	512 kbit/s-TDM/BPSK (+ FEC 1/2)	

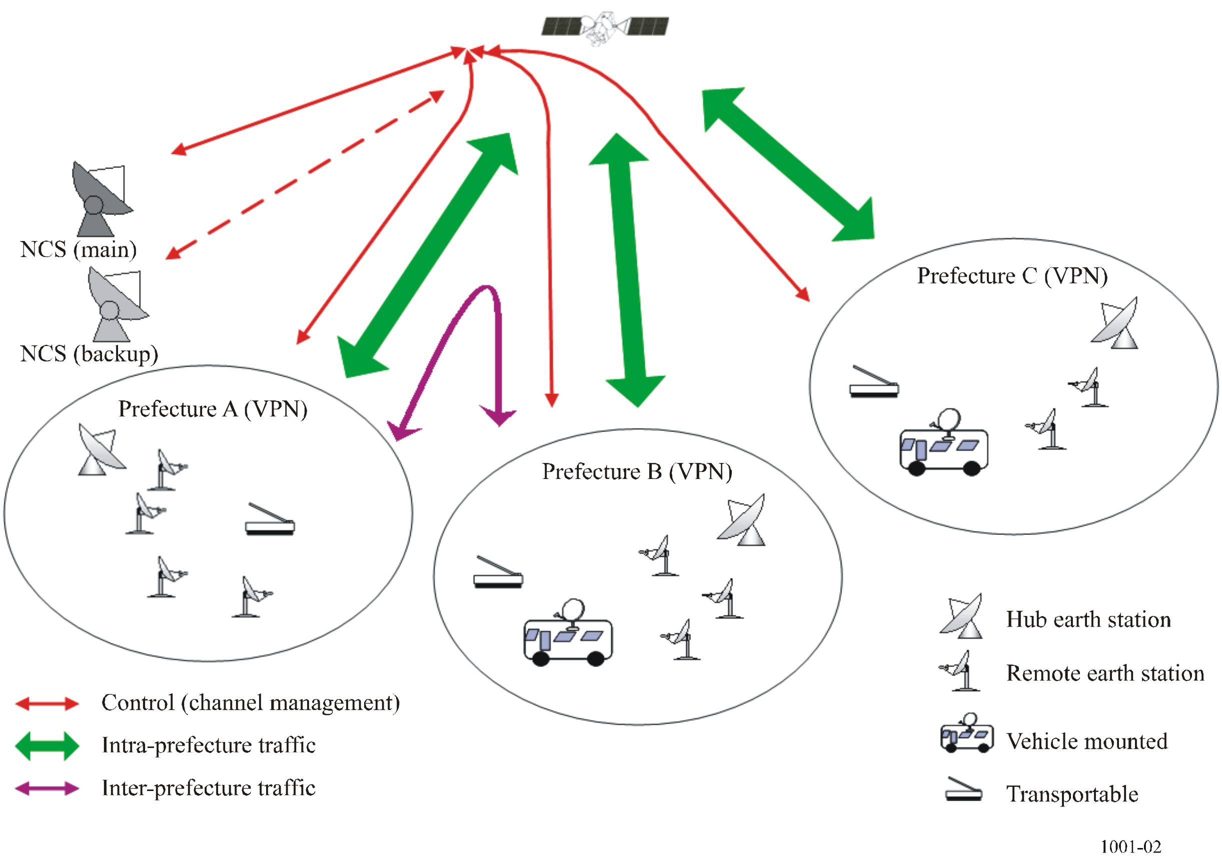
2.2 Example of an emergency network in Japan using the 14/12 GHz band

In Japan, there is a satellite network operating in the 14/12.5 GHz frequency band mainly for the purpose of emergency communications that accommodates more than 4 700 earth stations including VSATs located at municipal offices and fire departments, transportable earth stations and vehicle-mounted earth stations. The network provides voice, facsimile, announcement (simplex), video transmission and high-speed IP data transmission.

As shown in Fig. 2, the network is based on DAMA so that satellite channels can be efficiently shared by as many as 5 000 earth stations. An earth station asks the network coordination station (NCS) for the assignment of traffic channels such as voice, facsimile and IP transmission prior to its communication with other earth stations. Note that there are two NCSs, main and backup, in the network.

FIGURE 2

Configuration of the emergency network



The network is designed to have a multi-star topology where each prefecture (note that Japan consists of 47 prefectures) configures an independent sub-network so that the principal office of the prefecture can be the hub of emergency communications in the case of an event. By virtue of the closed-group network, the satellite resources can be controlled by the NCS depending on urgency of events. For instance, the NCS can provide priorities for communications originated from a particular prefecture where an emergency event occurs over routine communications in other prefectures. The network also provides inter-prefecture communications if any.

The summary of channel parameters is listed in Table 7. There are six types of channels consisting of SCPC (voice/data/fax), announcement, IP data transmission, digital video, satellite data broadcast and common signalling channel (CSC). SCPC channels (32 kbit/s ADPCM) and IP data transmission channels (32 kbit/s-8 Mbit/s variable rate) are assigned to earth stations on a demand basis by the NCS. The bandwidth of an IP data transmission channel is requested from an earth station based on its instantaneous throughput of IP data traffic and assigned by the NCS. Thus, the NCS manages the satellite resource efficiently by accommodating traffic channels with variable bandwidth by a novel channel management algorithm. An earth station designated to high-speed TCP/IP transmission is equipped with a 2-segment splitting TCP gateway to enhance the TCP throughput (see Recommendation ITU-R S.1711).

TABLE 7

Summary of channel parameters of the satellite network

Parameters	SCPC (voice, fax, data)	Announcement	IP data transmission	Digital video transmission	Satellite data broadcast	CSC
Direction	2-way	2-way	2-way	1-way	1-way	2-way
Multiple access(1)	DA-FDMA	PA-TDMA/FDMA	DA-FDMA	DA-FDMA	DA-FDMA	RA-TDMA/ FDMA
Modulation	QPSK (2)	QPSK(3)	QPSK	QPSK	QPSK	QPSK (3)
Information rate	32 kbit/s	32 kbit/s	32 kbits- 8 Mbit/s (4)	7.3 Mbit/s	6.1 Mbit/s	32 kbit/s
FEC	1/2 FEC	1/2 FEC	1/2 FEC (5)	3/4 FEC + RS	3/4 FEC + RS	1/2 FEC
Ciphering	N/A	N/A	(IPSec) (6)	(MULTI2)(6)	MISTY	N/A
Encoding	32 kbit/s ADPCM	32 kbit/s ADPCM	N/A	MPEG2	N/A	N/A

(1) The following are acronyms of multiple access schemes:
DA-FDMA: Demand assignment – frequency division multiple access
PA-TDMA: Permanent assignment – time division multiple access
RA-TDMA: Random access – time division multiple access
(2) The burst channel is employed because of voice activation.
(3) The burst channel is employed in the uplink direction.
(4) Asymmetric type variable rate with IP
(5) 3/4 FEC + RS is employed for channels over 3 Mbit/s.
(6) Optional.

In order to help communications from/to an area damaged by disasters, the development of smaller user earth stations with high performance is under way. Typical parameters of such earth stations are listed in Table 8. There are two types of vehicle-mounted earth stations. Type-A earth station is designed to transmit full motion picture based on MPEG-2 (i.e. 6 Mbit/s) and provide a voice circuit simultaneously available during video transmission. The earth station is to be mounted on a relatively large vehicle such as “Wagon” type. On the other hand, a type-B earth station is designed to transmit a low rate limited-motion picture by MPEG-4/IP (i.e. 1 Mbit/s) with a voice circuit switchable with video transmission. The earth station is to be mounted on a smaller vehicle such as “Land-cruiser” type. Similar to type-B vehicle-mounted earth stations, the transportable earth station is designed to transmit a low rate limited-motion picture by MPEG-4/IP with a voice circuit switchable with video transmission. Its video transmission rate is only 256 kbit/s.

TABLE 8

Parameters of the vehicle-mounted and transportable earth station

Parameters	Vehicle-mounted earth station		Transportable earth station
	Type-A	Type-B	
Description	– Full-motion pictures based on MPEG-2 – Simultaneous voice circuit	– IP-based low-rate motion picture based on MPEG-4 – Voice circuit switchable with the video circuit	– IP-based low-rate motion picture based on MPEG-4 – Voice circuit switchable with the video circuit
Antenna diameter	1.5 m (offset parabola)	75 cm (offset parabola)	1 m (Flat array)
Output power	70 W (SSPA)	15 W (SSPA)	15 W (SSPA)
Number of channels and transmission rate	Video: 1 channel (6 Mbit/s, MPEG-2) Voice/IP: 1 channel	Video: 1 channel (1 Mbit/s, IP) Voice/IP: 1 channel	Video: 1 channel (256 kbit/s, IP) Voice/IP: 1 channel
Type of vehicle	Wagon type	Land-cruiser type	N/A

2.3 Example of an emergency network in South-East Asia using the 14/12 GHz band

An agency in South-East Asia has set up an end-to-end broadband VSAT system to improve the broadband telecommunication between its offices and enhance the e-risk management policy.

The satellite network interconnects the headquarters (redounded) with: 13 national offices, 25 county offices, 72 villages and 12 emergency vehicles. Based on IP, it offers all the common services of an intranet such as access to web and FTP servers, electronic messaging and content distribution in multicast, e.g. streaming. In addition, it offers broadband applications relevant for crisis management (e-risks services suite): videoconferencing, collaborative working and voice-over-IP.

In normal situations, the system carries up to 8 Mbit/s:

– 2 Mbit/s shared by all voice communications;

– 3 Mbit/s for central data exchanges;

– 3 Mbit/s for data shared by other data exchanges.

In crisis situations, the system carries up to 21 Mbit/s:

– 12 Mbit/s for two video streams;

– 9 Mbit/s for up to 16 videoconference terminals.

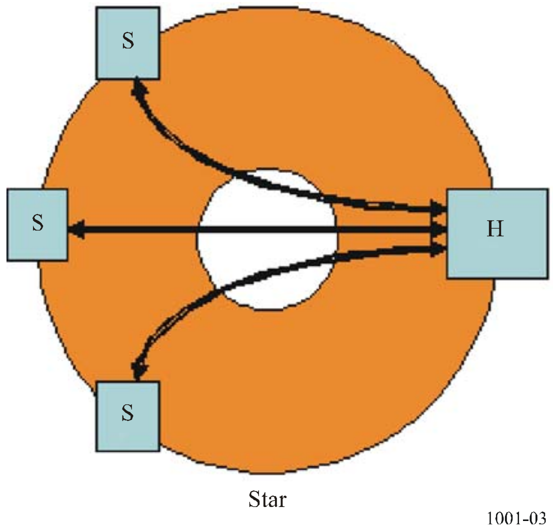
It is based on a DVB-RCS star satellite network. RCS stands for return channel by satellite. This technology corresponds to the standard EN 301 790 and enables access to multimedia services by satellite by the means of a small dish. It is cited in the Recommendation ITU-R S.1709 – Technical characteristics of air interfaces for global broadband satellite systems.

The topology chosen is the star topology (as opposed to the mesh one) with a hub installed at the headquarters and satellite terminals installed at the remote sites listed above.

This topology is the best suited to services such as videoconferencing since they are by nature point-to-multipoint with a multipoint control unit located at the hub. This one also enables access to the Internet by means of a broadband access server. It shall be located abroad from the place of the disaster, and therefore there is less constraint on the facilities; for example, the antenna can be as large as necessary.

FIGURE 3

Star topology



The network operates in 14/12 GHz band (the 14 GHz band for the uplinks; the 12 GHz band for the downlinks). 14/12 GHz band antennas are smaller and lighter, which eases the use and the transportation of material. The terminals are state-of-the-art with a diameter ranging from 0.6 m to 1.2 m; the diameter is chosen so as to optimize the trade-off between the signal-to-noise ratio and the ease of transportation. The RF subsystem of remote terminals is specified in the norm as the outdoor unit.

The forward link is compliant with the DVB-S standard implying QPSK modulation and a combination of a Reed-Solomon (188, 204) code as the outer code and a convolutional 1/2 code as the inner code. The protocol stack for the forward link is IP/MPE/MPEG2-TS/DVB-S[1].

The return link relies on QPSK modulation and a 2/3 turbo code. The protocol stack for the return link is IP/AAL5/ATM/DVB-RCS.

The satellite access technology on the return link is fixed multifrequency time division multiple access (fixed MF-TDMA). Fixed MF-TDMA allows a group of satellite terminals to communicate with the hub using a set of carrier frequencies of equal bandwidth while the time is divided into slots of equal duration. The network control centre at the hub will allocate to each active satellite terminal series of bursts, each defined by a frequency, a bandwidth, a start time and a duration.

The satellite network supports quality of service thanks to standard features at the MAC level: the so-called capacity categories; but the architectures enables the definition of a QoS policy at higher levels such as DiffServ or InterServ based policies (DiffServ is generally preferred).

Satellites terminals can be controlled from the hub, they can be configured, faults can be detected and software can be downloaded.

---

1 MPE stands for MultiProtocol Encapsulation.

RECOMMENDATION ITU-R M.1042-3

Disaster communications in the amateur and amateur-satellite services

(Question ITU-R 48/8)

(1994-1998-2003-2007)

Scope

This Recommendation provides guidance on the development of amateur and amateur-satellite service networks supporting preparedness and radiocommunications during disaster and relief operations.

The ITU Radiocommunication Assembly,

considering

a) Resolution 36 of the Plenipotentiary Conference (Kyoto, 1994);

b) Resolution 644 (Rev.WRC-2000) concerning telecommunications resources for disaster mitigation and relief operations;

c) the entry into force of the Tampere Convention on the provision of telecommunications resources for disaster mitigation and relief operations by the Intergovernmental Conference (1998) on 8 January 2005;

d) ITU-D Resolution 34 (Doha, 2006) (Rev. WTDC-06) on telecommunication resources in the service of humanitarian assistance;

e) Recommendation ITU-D 13.1 (Geneva, 2006) regarding effective utilization of the amateur services in disaster mitigation and relief operations;

f) that No. 25.9A of the Radio Regulations states that administrations are encouraged to take the necessary steps to allow amateur stations to prepare for and meet communication needs in support of disaster relief;

g) that the amateur service provides valuable training for radio operators,

recommends

1 that administrations encourage the development of amateur service and amateur-satellite service networks capable of providing radiocommunications in the event of natural disasters;

2 that such networks be robust, flexible and independent of other telecommunications services and capable of operating from emergency power;

3 that amateur organizations be encouraged to promote the design of robust systems capable of providing radiocommunications during disasters and relief operations.

RECOMMENDATION ITU-R F.1105-2*

Fixed wireless systems for disaster mitigation and relief operations

(Question ITU-R 239/9)

(1994-2002-2006)

Scope

This Recommendation provides characteristics of fixed wireless systems used for disaster mitigation and relief operations. Several types of such systems including transportable equipment are specified according to channel capacity, operating frequency bands, transmission distance and propagation path conditions.

Detailed descriptions of these systems are also given in Annex 1 as guidance.

The ITU Radiocommunication Assembly,

considering

a) that rapidly deployable telecommunications are essential for disaster mitigation and relief operations in the event of natural disasters, epidemics, famines and similar emergencies;

b) that measures to mitigate the effects of natural disasters should be made as much as possible;

c) that high speed data and high capacity information are available due to the popularity of fibre-to-the-home, digital subscriber line, mobile phones etc. in the form of voice, character data, image, or through a variety of Internet Protocol (IP)-based services;

d) that transportable fixed wireless equipment may be used for relief operation of either radio or cable links and may involve multi-hop applications with digital and analogue equipment;

e) that fixed wireless equipment for disaster mitigation and relief operations may be operated in locations with differing terrain and in differing climatic zones, uncontrolled environmental conditions and/or unstable power sources;

f) that fixed wireless equipment for disaster mitigation and relief operations may be used in areas with an unfavourable interference environment;

g) that interoperability and internetworking between fixed wireless system for disaster mitigation and relief operations and other networks would be beneficial in emergency situations as stated in *considering* a);

h) that efficient use of spectrum is required,

recognizing

a) that the World Radiocommunication Conference (WRC-03) invites ITU-R to continue its technical studies and to make recommendations concerning technical and operational implementation, as necessary, for advanced solutions to meet the needs of public protection and disaster relief radio-

* This Recommendation should be brought to the attention of Radiocommunication Study Group 8 (Working Party 8A) and Telecommunication Development Study Group 2.

communication applications, taking into account the capabilities, evolution and any resulting transition requirements of the existing systems, particularly those of many developing countries, for national and international operations (see the relevant part of Resolution 646 (WRC-03)),

recommends

1 that for disaster mitigation and relief operations in devastated areas or restoration of a break in transmission links the following types of fixed wireless systems as given in Table 1 should be considered;

TABLE 1

Types of fixed wireless systems for disaster mitigation and relief operations

Type	Feature	Application
A	A simple wireless link which can be established rapidly for telephone communication with a governmental or international headquarters	(1) (2)
B	One or more local networks which connect a communications centre and up to about 10 or 20 end-user stations with telephone links	(1)
C	A telephone link for between about 6 and 24 channels or a data link up to the primary rate over a line-of-sight or near line-of-sight path	(1) (2)
D	A link over an obstructed or trans-horizon path	(2)
E	A high-capacity telephone link (more than 24 channels) or digital fixed wireless link (above the primary rate)	(2)
F	Simultaneous individual or group radiocommunications using point-to-multipoint individual radiocommunications between a central station and a number of terminals in a region	(1), (3)

Types A to E: transportable system
Application (1): for devastated areas
Application (2): for breaks in transmission links
Application (3): for mitigation of disaster effects

2 that frequency bands used for fixed wireless systems for disaster mitigation and relief operations described in Table 1 should be in accordance with the Radio Regulations for the fixed service, as well as with national and regional frequency allocations (see Table 2);

3 that radio-frequency arrangements for fixed wireless systems for disaster mitigation and relief operations in the chosen bands should be in accordance with ITU-R Recommendations (see Recommendation ITU-R F.746) and national standards;

4 that interconnection of transportable fixed wireless systems with analogue and digital cable systems at repeater stations should be made at baseband;

5 that interconnection of transportable fixed wireless systems with fibre-optic systems at repeater stations may be made at points with a significant level of optical power;

6 that for system characteristics, the information contained in § 1 of Annex 1 can be referred to as a guide for administrations and system planners;

7 that performance objectives of links which use transportable fixed wireless equipment as well as separate links formed by the transportable fixed wireless equipment during restoration should have transmission performance values sufficient for normal service (see § 3 of Annex 1);

8 that transportable fixed wireless systems, Types A to E in Table 1 including Annex 1 describing their characteristics, should be used for the access link to a base station in mobile communications that are operating in disaster relief and emergency situations.

Annex 1

Descriptions of fixed wireless systems for disaster mitigation and relief operations

1 System characteristics

For each type of system in Table 1, the channel capacities, frequency bands and path distances given in Table 2 are suitable.

TABLE 2

Basic characteristics

System type	Capacity	Example frequency bands [1]	Transmission path distance
A	1-2 channels	HF (2-10 MHz)	Up to 250 km and beyond
B	Local network with 10-20 outstations (several channels)	VHF (50-88 MHz) (150-174 MHz) UHF (335-470 MHz)	Up to a few km
C	From 6 to 120 channels 1.5/2 or 6.3/8 Mbit/s	UHF (335-470 MHz) (1.4-1.6 GHz) SHF (7-8 GHz) (10.5-10.68 GHz)	Up to 100 km
D	From 12 to 480 channels 1.5/2, 6.3/8, 4 × 6.3/8 Mbit/s or 34/45 Mbit/s	UHF (800-1 000 MHz) (1.7-2.7 GHz) SHF (4.2-5 GHz)	Line-of-sight or obstructed paths
E	960-2 700 FDM channels STM-0 (52 Mbit/s) or STM-1 (155 Mbit/s)	SHF (4.4-5 GHz) (7.1-8.5 GHz) (10.5-10.68 GHz) (11.7-13.2 GHz) (23 GHz)	Up to several tens of km
F	6-TDMA channels e.g. up to 2 000 individual calls e.g. up to 200 group calls	VHF (54-70 MHz)	Up to 10 km (typical) Extension with repeater(s)

FDM: frequency division multiplexing

TDMA: time division multiple access

STM: synchronous transfer mode

(1) Many parts of these bands are shared with satellite services.

In the case of links to an earth station operating in a satellite service, the following additional restrictions should be considered:

– space-to-Earth frequency bands should be avoided;
– problems could arise if Earth-to-space frequency bands are used;
– trans-horizon systems (Type D) should be avoided.

It would be preferable to avoid bands likely to be in use or planned for trunk communications. However, these bands may be used for Type E with careful consideration of interference problems by the administration.

2 Engineering principles

2.1 Low-capacity links (Type A system)

HF transportable equipment for 1 or 2 channels should employ only solid-state components and should be designed to switch off the transmitters when not in use, in order to conserve battery power, and to reduce the potential of interference.

As an example, a solid-state 100 W single-sideband terminal in a band between, say, 2 and 8 MHz operated with a whip antenna, could have a range of up to 250 km. Simplex operation (transmitter and receiver employing the same frequency) with a frequency synthesizer to ensure a wide and rapid choice of frequency when interference occurs and to facilitate setting-up in an emergency, can give up to 24 h operation from a relatively small battery (assuming that use of the transmitter is not excessive). The battery can be charged from a vehicle generator and all units can be hand-carried over rough country.

2.2 Local radio networks (Type B system)

Radio networks of Type B are envisaged as local centres with single-channel radiocommunication with 10 to 20 out-stations, operating on VHF or UHF up to about 470 MHz. Single-channel and multi-channel equipments similar to types used in the land mobile service could be used.

2.3 Links up to 120 channels (Type C system)

Equipment which is suitable for transportation by road, railway or helicopter is available. Such equipment, together with power supply equipment, can be easily and quickly installed and put into service. The equipment capacity is from about 1.5/2 to 6.3/8 Mbit/s, depending on the requirements, the topography and other factors.

d.c. operated equipment or a.c. powered equipment automatically switchable to d.c. is preferred. It can be associated with light-weight, high gain Yagi or grid antennas, giving a range of up to 100 km line-of-sight, but capable of accepting some obstruction from trees on shorter paths. Simply erected guyed or telescopic poles which can be rotated from ground level are to be preferred. If separate antennas are used for transmitting and receiving with cross-polarization, it is convenient for the transmitters to be connected to antennas which are polarized at 45° (from top right to bottom left looking along the path from behind the antenna); if transmit and receive antennas are mounted on the same sub-assembly, with male and female connectors, there can then be no confusion over the plane of polarization to be selected, since the received signal will always be cross-polarized with respect to the transmitted one.

Single frequency, or selectable pre-set frequencies are to be preferred to eliminate as many variables as possible during the initial setting-up of the equipment. The ability to appropriately select transmit and receive frequencies in the field over a wide frequency band is an advantage. Foam-filled or solid dielectric flexible cable is to be preferred as this is less liable to mechanical damage and the effects of moisture.

2.4 Links up to 480 channels (Type D system)

Equipment which is suitable for transportation by road or railway or by helicopter is available. Such equipment, together with power supply equipment, can be easily and quickly installed and put into service. The equipment capacity is from about 12 to 480 telephone channels, depending on the requirements, the topography and other factors. The use of receivers with low noise factors and with special demodulators and of diversity reception, enables the size of the antennas, the transmitter power and the size of the power supply equipment, to be smaller than those often used for conventional trans-horizon installations.

In line-of-sight or partially obstructed path conditions, transportable equipment with similar fast deployment capability but with transmission capacities of up to 34/45 Mbit/s is available. d.c. operated equipment or a.c. powered equipment automatically switchable to d.c. is preferred. It can be associated with light-weight grid antennas, giving a range of line-of-sight, but capable of accepting some obstruction from trees on shorter paths. Simply erected guyed or telescopic poles which can be rotated from ground level are to be preferred.

The ability to appropriately select transmit and receive frequencies in the field over a wide frequency band is an advantage.

2.5 High capacity links (Type E system)

For higher frequency bands and capacities of 960 telephone channels and above, it is recommended that the radio-frequency equipment is integrated directly to the antennas. For transportable equipment, preference should be given to equipment in which reflectors of diameter less than about 2 m are available. Because IF interconnection at repeaters is a desirable feature, an IF interconnection should be possible between the radio-frequency heads.

However, since the equipment which is to be bypassed in an emergency or for temporary use will most likely be at ground level, the control cable should bring the IF to the control unit at ground level. The antennas of systems used for relief operations are likely to be smaller than those of fixed microwave links and it is therefore important that the output power of the transmitters should be as high as possible and the noise factor of receivers should be as low as possible. Battery operated equipment is preferable: 12 V and/or 24 V supplies are appropriate if the batteries are to be rechargeable from the dynamos or alternators of any vehicles which are available.

An alternative arrangement would be to house the equipment in a number of containers. These would not only facilitate the transport of the equipment but each container could provide facilities for rapidly installing a number of transmitters and receivers. The maximum number of transceivers to be housed in any one container would depend on the dimensions and maximum weight adopted, allowing for transport by helicopter, aeroplane or any other means of transport. Furthermore, it is preferable to take into consideration equipment operating with ordinary commercial power supplies. Fixed wireless systems generally require line-of-sight operation. For digital fixed wireless systems, the interface should be based on the primary rate (2 Mbit/s (E1) or 1.5 Mbit/s (T1)).

2.6 Regional simultaneous communication system (Type F system)

This type operates as a point-to-multipoint system in ordinary time, and, in case of emergency, works in particular for disaster relief communications.

A central station (CS) in a local/municipal office usually provides public information to outdoor terminal stations (OS) or indoor receivers for daily communications between the office and residents. The CS also collects data or information for potential prevention of disasters from OS through the monitoring camera, telemeter, etc., or from disaster prevention systems used in other districts. The above information may include meteorological data or notice of storms and fires. These usual communications are performed in TDMA-TDD.

For OSs far from the CS, a repeater station (or more than one station in series) can be deployed. Repeater stations may work as an OS with a function of interactive communication.

In the case that a disaster occurs or is likely to occur, the CS transmits necessary information or warnings for storm, earthquake or tsunami to the residents by means of loudspeakers or character displays that are equipped with the OS and indoor receiver. This downlink information is transmitted in simultaneous distribution mode.

Interactive communications between the CS and an individual OS is possible even when simultaneous distribution is under way, using other time slots in TDMA-TDD. Thus, important information from the damaged area can be efficiently transmitted to the CS, including relief operation status, urgently required resources or residents' safety information.

For further information, see Appendix 1.

3 Transmission performance

Systems of Type A will have a noise performance which is critically dependent upon the antennas and path length in a particular case.

Systems of Types B and C are likely to provide similar transmission quality, when in use for relief work, as in normal use. A minimum sustainable $< 1 \times 10^{-8}$ BER objective can be used as guidance for digital systems.

Systems of Type D would, as with Type A, be very dependent upon the sitting of the terminals and the size of antennas. A minimum sustainable $< 1 \times 10^{-8}$ BER objective can be used as guidance for digital systems.

Transportable microwave equipment of Type E, because of the need to use smaller antennas and lower transmitter powers than for fixed links, would be likely to have a transmission quality below that normally required for trunk connections. Nonetheless this performance should be such that the network can still carry out all normal functions. Guidance for the performance in such emergency conditions is given as follows:

- < 1 000 pW for up to 50 km for 960 channels (4-12 GHz);
- < 5 000 pW for up to 50 km for more than 1 800 channels (4-6 GHz);
- < 5 000 pW for up to 25 km for 2 700 channels (11 GHz);
- $< 1 \times 10^{-8}$ BER for digital systems.

System of Type F requires:

- $< 1 \times 10^{-3}$ BER for indoor receiver terminals.
- $< 1 \times 10^{-4}$ BER for outdoor terminals with loudspeakers.

Appendix 1
to Annex 1

Features and applications of Regional Digital Simultaneous Communication System for disaster prevention and relief operations

Regional Digital Simultaneous Communication System (RDSCS) based on ARIB STD-T86* has been developed for disaster prevention and relief operations, that is, for collection of data or information for prevention of disaster or damage by disaster, and for transmission of necessary information or alarm to the residents, besides for voice or data communications between the central office and residents.

Locating a central station in the local office and a number of terminals in the region, the system provides simultaneous or group communications besides point to multipoint individual communications between the central station and the terminals.

The central station collects data or information for prevention of or damage by disasters; from monitoring cameras, telemeters, human, etc. through the outdoor terminals using TDMA, or from other disaster prevention system through telephone or facsimile. Then the central station transmits necessary information or alarm to the residents through the outdoor terminals and the indoor receivers by means of loudspeakers or character displays with simultaneous distributing mode.

Each outdoor terminal is capable of interactive communications with the central station by TDD mode. 6-time slots TDMA can provide individual communication even during the time where simultaneous distribution is under way.

Up to 2 000 individual calls or up to 200 group calls can be made through 6-TDMA channels, though these capacities depend upon manufactures model.

Through 16-QAM scheme, 45 kbit/s transmission speed is possible with 15 kHz radio channel separation, providing image data collection at the central station, and character display at the terminals.

For terminals far from the central station, a repeater that provides dropout function is installed, enabling terminals to access to a repeater as well as to the central station. Two or more repeaters could be installed in series if necessary. By adopting the repeaters, transmitter power output of each outdoor terminal could become 10 W or less. Together with TDD and TDMA operations, low power consumption of the outdoor-terminal makes it possible to use solar power supply or hybrid of solar and wind generator.

In this standard interoperability between terminals or systems of different suppliers is assured, enabling such equipment in other areas to be brought to the disaster area for relief operations.

In ordinary times, the system is utilized for warning of storm, fire, etc., as well as daily communications between the local office and residents.

Summary of technical specifications:

Frequency band:	54-70 MHz
Channel separation:	15 kHz
Transmitter power:	10 W or less
Transmission speed:	45 kbit/s
Modulation scheme:	16-QAM
Communication method:	TDMA-TDD
Voice CODEC:	16 kbit/s high efficiency voice CODEC for loudspeaker operation.

* www.arib.or.jp/english/html/overview/itu/itu-arib_std-t86v1.0_e.pdf.

RECOMMENDATION ITU-R M.1467-1*

Prediction of sea area A2 and NAVTEX ranges and protection of the A2 global maritime distress and safety system distress watch channel

(Question ITU-R 92/8)

(2000-2006)

Scope

Recommendation ITU-R M.1467 provides guidance to administrations for predicting sea area A2 and NAVTEX coverage areas by taking into account variations in the propagation conditions. These coverage areas can be confirmed by measurement. This information is provided for administrations that are upgrading, or planning to upgrade, their shore-based facilities for global maritime distress and safety system (GMDSS) operation in the A2 sea area.

The ITU Radiocommunication Assembly,

considering

a) that the International Convention for Safety of Life at Sea (SOLAS) 1974, as amended, prescribes that all ships subject to this Convention shall be fitted for the global maritime distress and safety system (GMDSS) by 1 February 1999;

b) that some administrations have yet to establish A2 services for the GMDSS;

c) that Question ITU-R 92/8 identifies the need for promulgation of minimum performance criteria for the protection of the service, and guidance to accelerate the upgrade of shore-based facilities for GMDSS operation in the A2 sea area,

recommends

1 that administrations currently upgrading, or planning to upgrade, their shore-based facilities for GMDSS operation in the A2 sea area should base such upgrading on the information contained in Annex 1. Administrations are invited to develop appropriate software to perform the calculations described in Annex 1.

Annex 1

Prediction of A2 and NAVTEX ranges

1 Overview

In order to establish a new A2 sea area it is necessary to account for variations in the propagation conditions. A2 coverage is by groundwave, which is largely stable, enabling the extent of the service area to be confirmed by measurement, as is recommended by the IMO, before committing capital expenditure.

The design criteria to be used for establishing A2 and NAVTEX sea areas are defined by the IMO in Annex 3 to their Resolution A.801(19).

* This Recommendation should be brought to the attention of the International Maritime Organization (IMO).

2 Prediction of A2 and NAVTEX ranges

2.1 IMO performance criteria

The criteria developed by the IMO for determination of A2 and NAVTEX ranges are reproduced in Table 1 and should be used in the determination of ranges for A2 and NAVTEX services.

TABLE 1

Performance criteria for A2 and NAVTEX transmissions

Distress channel	Radiotelephony	DSC	ARQ NBDP	NAVTEX
Frequency (kHz)	2 182	2 187.5	2 174.50	490 and 518
Bandwidth (Hz)	3 000	300	300	300
Propagation	Groundwave	Groundwave	Groundwave	Groundwave
Ship's power (W)	60	60	60	
Ship's antenna efficiency (%)	25	25	25	25
RF full bandwidth signal/noise ratio (S/N) (dB)	9	12	18 min(1)	8
Mean Tx power below peak (dB)	8	0	0	0
Fading margin (dB)	3	Not stated		3
IMO reference for above	Res. A.801(19)	Res. A.804(19)	Rec. ITU-R F.339	Res. A.801(19)
Availability required (%)	95(2)	Not stated	Not stated	90

DSC: digital selective calling

NBDP: narrow-band direct printing

(1) Stated as 43 dB(Hz) under stable and 52 dB(Hz) under fading conditions with 90% traffic efficiency.

(2) Availability can be relaxed to 90% in cases where the noise data used or performance achieved can be proven by measurement.

2.2 Achieving the required quality of signal

2.2.1 The effect of received noise

On a very quiet site, man-made noise dominates below 4 MHz and galactic noise above. These combine, at the receive antenna with seasonal levels of atmospheric noise, and also transmitter sideband noise, as shown in Fig. 1. Recommendation ITU-R P.372 should be used to account for atmospheric and normal man-made noise levels.

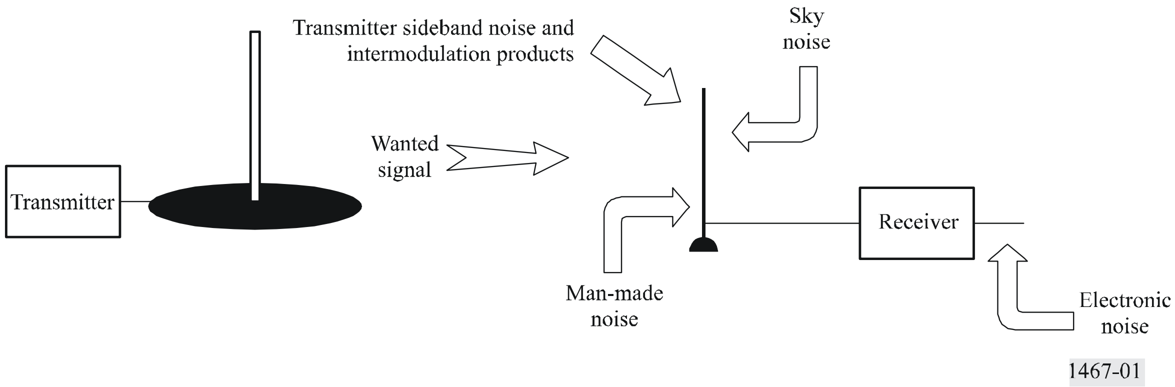
Paragraph 3.5 should be used to ensure that the levels of transmitter sideband noise and intermodulation products reaching the receive antenna by groundwave do not exceed the tolerable limit for protection of the A2 DSC watch frequency.

2.2.2 C/N required for single sideband (SSB) radiotelephony

In order to maintain the intelligibility of a received SSB radiotelephony signal it is necessary to provide the operator with a minimum AF signal/noise plus distortion ratio (SINAD), which in turn defines the RF C/N required at the receive antenna.

FIGURE 1

Determination of required carrier-to-noise ratio (*C*/*N*)



The capture range for an A2 receive system should be calculated assuming an RF *C*/*N* density figure of 52 dB(Hz) at the shore-based receive antenna. This will ensure that a ship's transmitter operating with a peak-to-mean ratio of 8 dB provides the shore-based operator with a 9 dB *S*/*N* in a 3 000 Hz bandwidth, as stipulated by the IMO.

The receive antenna and multicoupler should be designed to offer good linearity to minimize the risk of intermodulation products being generated on the watch frequencies. With good electronic design the noise generated within the receive system itself can be ignored below 3 MHz.

2.2.3 *C*/*N* required for NAVTEX broadcasts

The transmit range for NAVTEX broadcasts should be calculated assuming an RF *C*/*N* density figure of 35 dB(Hz) at the ship's antenna. This will ensure that the NAVTEX receiver is provided with an RF *S*/*N* of 8 dB in a 300 Hz bandwidth.

2.3 Accounting for ships topside noise

Topside noise refers to the environmental noise generated by ship-borne machinery, and other sources, and a figure is required for entry into NOISEDAT and other programs. Table 2 shows a number of published figures, and for reference purposes includes galactic and quasi-minimum noise levels, which is accepted as representing the best achievable noise floor.

TABLE 2

Naval environmental categories for topside noise

Environmental category	dB below 1 W ref. 3 MHz
DOD Cat 1 mobile platform	−137.0
IPS ship (ASAPS and GWPS)	−142.0
AGARD ship	−148.0
Quasi-minimum noise	−156.7
Noise galactic (Rec. ITU-R P.372)	−163.6

ASAPS: advanced stand alone prediction system

GWPS: groundwave prediction system

The Australian Department of Defence (DOD) and Advisory Group for Aeronautical Research and Development (AGARD) have both published relevant figures. The AGARD figure represents a naval vessel under normal cruise conditions, whilst the DOD figure represents the maximum level under battle conditions with all machinery in operation.

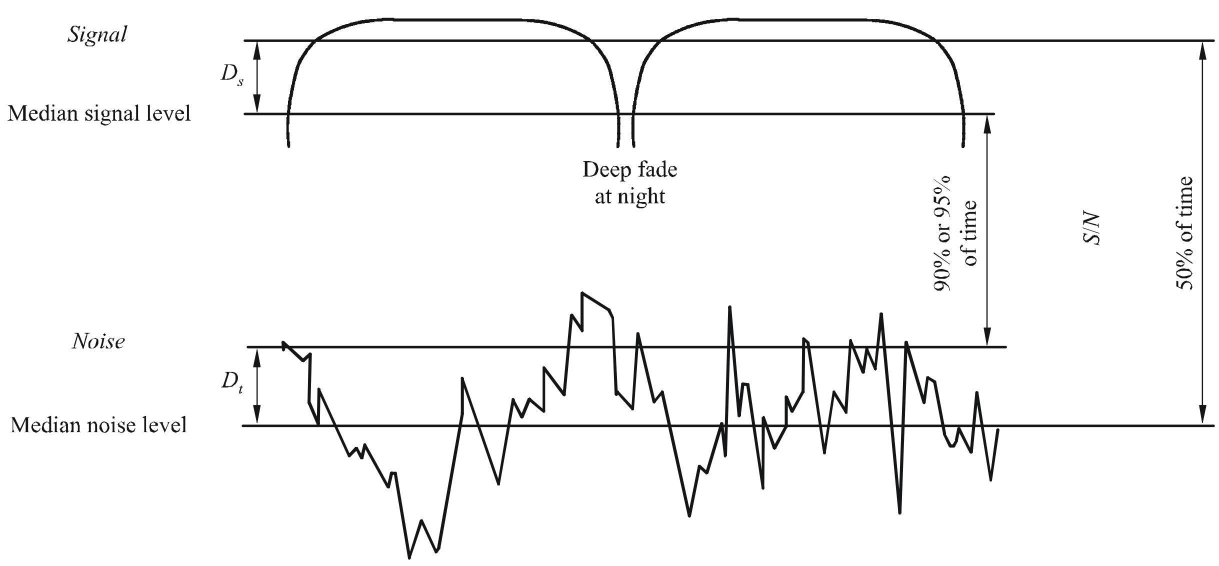
The levels of noise to be expected on commercial vessels can be expected to range between these figures. The IPS Radio and Space Services (IPS) of the Australian Department of Industry have adopted an intermediate figure in their GWPS, which is well accepted as representing the noise level encountered on container vessels, pleasure cruisers, and utility ships. This figure, −142 dBW, should be used in prediction of coverage area of shore-based GMDSS transmitters.

2.4 Determination of external noise factor, F_a, for the required availability

An A2 area in the GMDSS is defined as the area within which ship stations can alert shore stations by using DSC on MF and communicate with the shore stations using MF radiotelephony (class of emission J3E). The communications ranges for voice signals are shorter than for DSC and the IMO criteria for determination of A2 areas should therefore be based on the communication of voice signals.

The range achieved by a transmitter or a receiver depends upon the radiated power, the propagation loss, and the ability of the receiver to discriminate between the wanted signal and the unwanted noise or interference. The level of each component in the received signal will drift as the propagation conditions change with time, and therefore arrive at the receive antenna in varying proportions. The final system design should therefore ensure that the level of the signal will exceed the level of the noise by an adequate amount for an adequate proportion of the time. This proportion is called the availability, and is determined by quantifying the behaviour of the signal and the noise with time as shown in Fig. 2.

FIGURE 2



D_s: lower limit in signal level variation
D_t: upper limit in signal level variation

Equation (1) should be used to calculate an upper value F_a for the external noise factor which corresponds to the required availability:

$$F_a = F_{am} + \sqrt{D_t^2 + D_s^2} \qquad \text{dB above } k\,T_0\,B \qquad (1)$$

where:

F_{am}: median external noise factor

D_s: variation in signal level expected for the required time percentage, to which is ascribed the figure of 3 dB specified by the IMO as fading margin

D_t: variation in noise level expected for the required percentage of time.

90% availability is required for NAVTEX broadcasts, and so the upper decile value D_u should be substituted for D_t in equation (1).

95% availability is required for A2 coverage. To achieve this, substitute $D_t = D_u + 3$ dB in equation (1).

First F_{am} and D_u should be determined by running the Noise1 program, which comes with the ITU NOISEDAT package. The program requests seasons required, site location, frequency, level or category of man-made noise, and type of data output required (select F_a), local mean time, and statistical parameters required (select overall median). For prediction of external noise factor on ship stations, the reference figure of −142 dBW should be used to account for topside noise, if no better data is available.

The data is presented in seasonal blocks as shown in Table 3, the data fields being explained in Table 4.

TABLE 3

Sample NOISEDAT output

LAT = –51.45,			LONG = –57.56,	DUMMY SITE					
WINTER	FMHZ = 2.182,			QUIET RURAL NOISE					
			OVERALL NOISE						
TIME BLOCK	ATMO	GAL	MANMADE	OVERALL	DL	DU	SL	SM	SU
0000-0400	59.3	44.2	43.9	59.6	7.2	9.2	2.3	3.5	2.6
0400-0800	54.0	44.2	43.9	54.5	4.1	1.9	3.2	3.4	2.7
0800-1200	28.2	44.2	43.9	45.9	4.3	9.0	2.2	3.4	1.3
1200-1600	31.0	44.2	43.9	46.0	4.2	8.9	2.2	3.3	1.3
1600-2000	53.5	44.2	43.9	53.9	10.4	12.2	3.6	3.9	2.9
2000-2400	54.3	44.2	43.9	55.2	7.2	9.2	2.3	3.7	2.6

TABLE 4

Fields presented for use in the NOISEDAT output

Field	Symbol	Description
TIME BLOCK		Time block during which original measurements were made
ATMO		Level of atmospheric component
GAL		Level of galactic component
MANMADE		Level of man-made component
OVERALL	F_{am}	Median level of F_a
DL	D_l	Lower decile of deviation from median
DU	D_u	Upper decile of deviation from median
SL	σD_l	Standard deviation of D_l
SM	σF_{am}	Standard deviation of F_{am}
SU	σD_u	Standard deviation of D_u

The median and upper values for F_a should be organized as shown in Table 5, and the seasonal spread in the value of F_a for the required availability should be plotted as a bar graph in Fig. 3. This presentation enables the process to be reviewed if any anomalies occur.

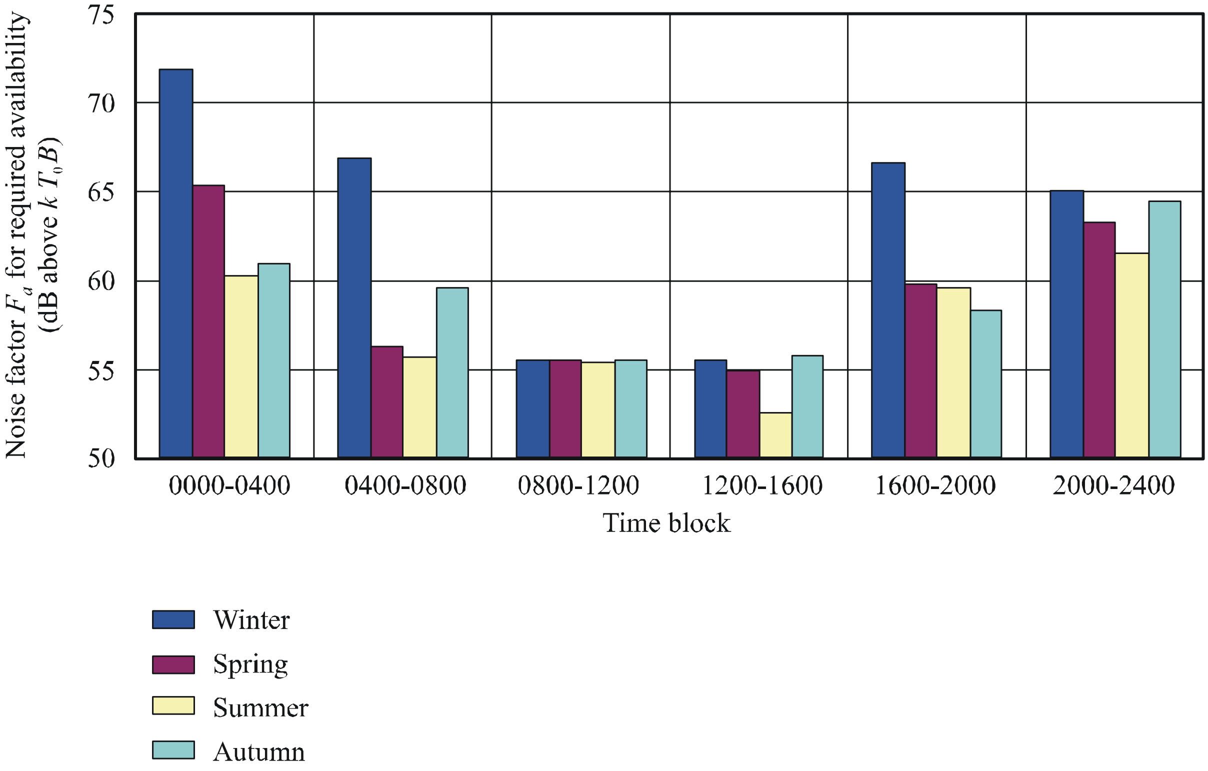
TABLE 5

External noise factor, F_a

	Median value, F_{am}				**F_a for required availability** $F_{am} + \sqrt{D_t^2 + D_s^2}$			
Time block	Winter	Spring	Summer	Autumn	Winter	Spring	Summer	Autumn
0000-0400	59.6	55.9	52	52.2	71.7	65.2	60.2	60.9
0400-0800	54.5	43.7	45.9	46	66.8	56.2	55.6	59.5
0800-1200	45.9	45.9	45.8	45.9	55.4	55.4	55.3	55.4
1200-1600	46	41.9	37.7	45.8	55.4	54.8	52.5	55.7
1600-2000	53.9	43.2	43.6	43.9	66.5	59.7	59.5	58.2
2000-2400	55.2	55	54.4	55.8	64.9	63.2	61.4	64.3

FIGURE 3

Seasonal spread in external noise, F_a, calculated for required availability



1467-03

IMO Resolution A.801(19) states "Administrations should determine time-periods and seasons appropriate to their geographic area based on prevailing noise levels".

2.5 Accounting for propagation by groundwave

2.5.1 Introduction

Horizontally polarized waves will not propagate along the surface of normal ground, as the electric vector runs tangential to the surface causing a current to flow, which results in absorption and heavy transmission losses. For this reason groundwaves have to be vertically polarized, and can only be generated by a vertical antenna, or to a limited extent by an antenna which is not perfectly horizontal, either because one end is higher than the other, or because the elements droop.

The prime mover for groundwave propagation is the cymomotive force (c.m.f.) exerted by the transmit antenna. In free space, power flux-density (W/m^2) decreases inversely with the square of distance, and so the field strength decreases inversely with distance and has a value equal to the product of c.m.f. and distance. The c.m.f. is synonymous with the effective monopole radiated power (e.m.r.p.), which is the power (kW) which would have to be fed into a short lossless monopole to achieve the same c.m.f., and in dB terms the two have the same value. A short lossless monopole on a perfect ground fed with 1 kW has a c.m.f. of 300 V, which is the reference used in the groundwave curves given in Recommendation ITU-R P.368.

Subsequent calculation of the transmitter power required should take account of the following losses associated with the antenna:

– the transmitter output power may be de-rated by an antenna offering a poor match;

– power will be absorbed by the ground and the feeder;

– whereas an ideal monopole will produce maximum radiation along the ground, the radiation from a real antenna will peak a few degrees above the ground and tuck in to a lower value along the ground.

2.5.2 Proof of performance tests

IMO Resolution A.801(19) stipulates that the range of the A2 sea area should be verified by field strength measurement. The c.m.f. of any shore-based transmitter and antenna should therefore be determined by operating the transmitter continuously at peak power, and measuring the resulting field strength using a portable field strength meter. This should be done on an arc around the station with an approximate radius of 1 km in the required directions of propagation. The precise location of the antenna and each measurement point should be fixed using a GPS navigator. The c.m.f. on each bearing is then the product of field strength (mV/m) and range (km) for each measurement point. The antenna drive point current should also be recorded before and after the measurement.

The procedures in this Recommendation should be used by administrations to determine the c.m.f. required to establish coverage, which should then be demonstrated by the equipment supplier, effectively eliminating uncertainties in performance due to local ground conditions, and the antenna and station earthing system.

2.5.3 Determination of extent of A2 service area

The extent of the A2 service area is determined by the range over which SSB communication is effective at 2 182 kHz between ship and shore. The ship is considered to be fitted with a 60 W transmitter, feeding a short monopole antenna with an efficiency of 25%, as given in Table 1.

The range is fixed by the maximum distance at which the ship can be from the shore station to produce an S/N of 9 dB in a 3 kHz bandwidth out of the receive antenna at the shore station. The shore transmit station must transmit sufficient power to return the same S/N at the output of the ship's receive antenna.

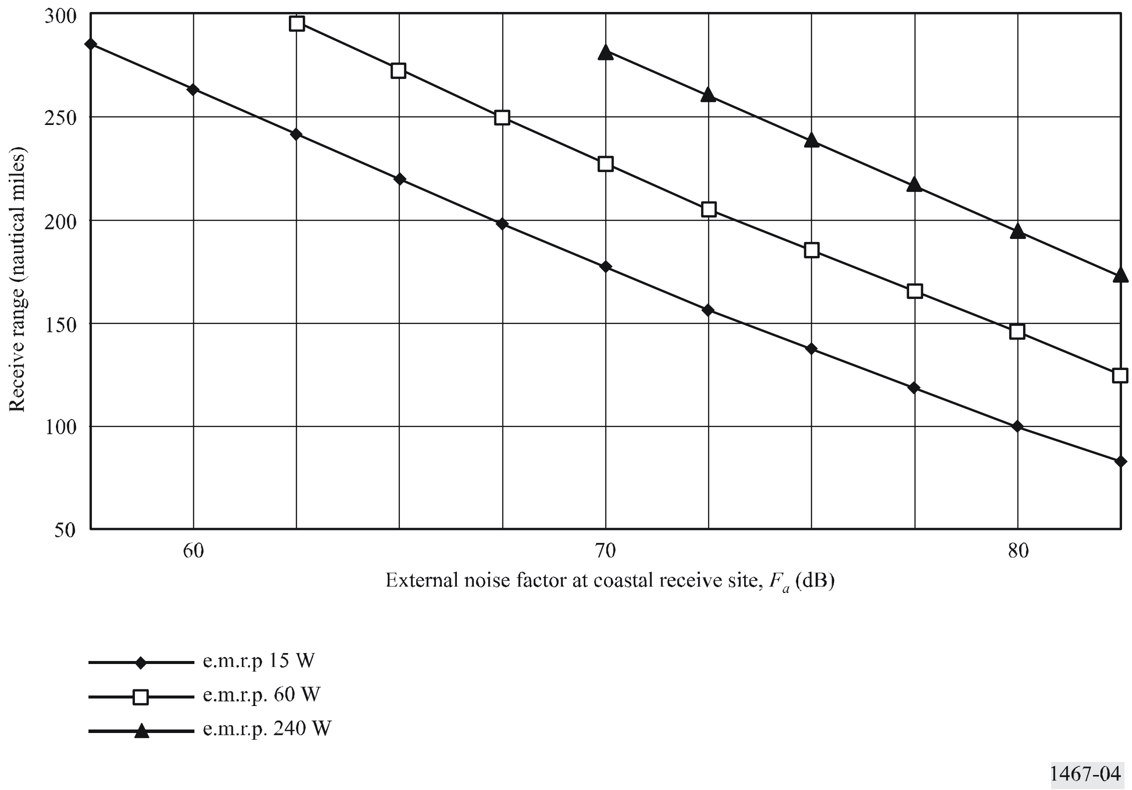
The range in both directions depends upon the sensitivity of the receive antenna, which depends upon the levels of natural and man-made noise present, and the ability of the antenna to discriminate between the wanted signal and the unwanted radiated noise. Although some improvement can be achieved by using a directional receive antenna, this often proves to be uneconomic and impractical, and is outside the scope of this Recommendation. It will be assumed that a short whip antenna is used for reception, that it has been installed on clear ground on an earth mat, and that it is regularly maintained to avoid the effects of corrosion. The noise factor of the receive system connected to the antenna can be ignored at 2 182 kHz.

2.5.3.1 Determination of shore-based receive range

The IMO minimum range thus achieved should be determined for all seasonal values of F_a using the 15 W curve in Fig. 4. Additional curves have been included to demonstrate the benefit of vessels using higher transmit powers.

FIGURE 4

Distress receive range versus F_a for various transmitted ships powers



2.5.3.2 Determination of shore-based transmit power required

Effective two-way SSB radiotelephony requires matched conditions in both directions. Since the transmission loss is the same in both directions the power required to return a call depends primarily upon the difference in noise levels at each end, and also the difference in transmit antenna efficiency. However the following additional factors have a direct impact on the power to be transmitted by the shore station:

– peaks and troughs in the radiation pattern of the receive antenna on the ship, due to interaction with the ship's hull;

– losses due to the condition of the ship's receive antenna on the ship.

Tests on scale models of a number of vessels indicate that variability in gain of receive antennas is typically ±5 dB. Furthermore, allowance should be made for ships whose antennas are in poorly maintained condition. A figure of 10 dB has been included in the calculation of shore-ship power budget to take account of these factors.

To determine the radiated power required from the shore-based transmitter the external noise factors for the receive stations on shore, F_{ac}, and ship, F_{as}, should first be established as described in § 2.4. The minimum e.m.r.p. required to return a GMDSS call at the same S/N to a ship on the limit of the service area should then be calculated using equation (2):

$$P_{e.m.r.p.} = (F_{as} - F_{ac}) - 16 + R_{pm} \qquad \text{dB(kW)} \qquad (2)$$

where:

R_{pm}: peak-to-mean ratio of the transmitter used on the shore station (dB).

The transmitter power required, P_{Tx}, should then be determined from equation (3), in which L_a should account for all the losses associated with the antenna described in § 2.5.1:

$$P_{Tx} = P_{e.m.r.p.} + L_a \tag{3}$$

Substituting typical figures $(F_{as} - F_{ac}) = 10$ dB, $R_{pm} = 3$ dB, and $L_a = 3$ dB yields a typical value of 1 000 W for the minimum required transmitter power at the coast station.

If the antenna efficiency Eff_{ant} is required it should then be determined from equation (4):

$$Eff_{ant} = P_{e.m.r.p.}/P_{Tx} \tag{4}$$

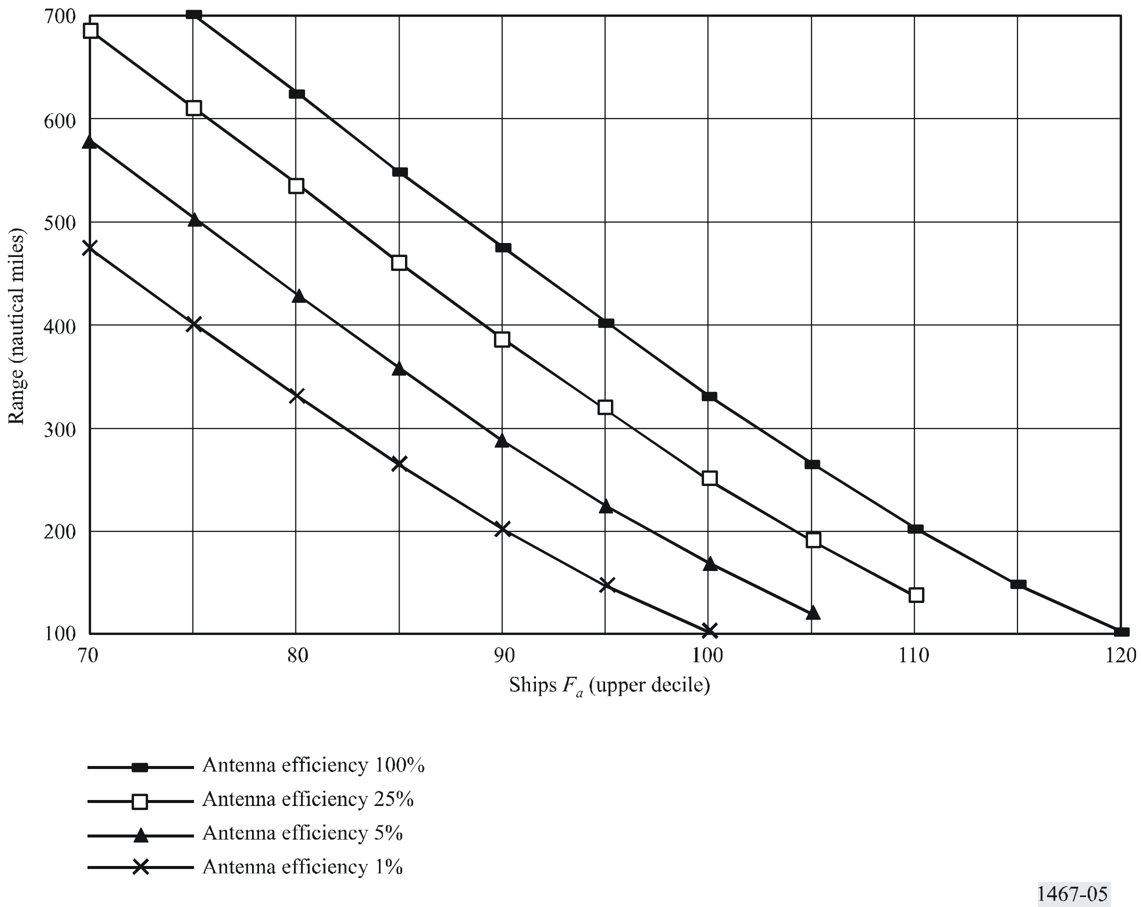
2.5.4 Determination of the range achieved using NAVTEX operation

The range achieved by a given NAVTEX transmitter depends upon the efficiency of the transmit antenna, and the external noise factor on board the ship, as shown in Fig. 5. The antenna efficiency depends upon the quality of the Earth system provided, and once the required c.m.f. has been determined, it should be measured as described in § 2.5.2, and the efficiency determined.

FIGURE 5

NAVTEX range for a 1 kW transmitter, versus ships F_a

(For 5 kW transmitter, reduce F_a by 7 dB)



IMO Resolution A.801(19) specifies 90% availability and so the upper decile value for F_a should be calculated using the statistical data produced by NOISEDAT.

3 Protection of A2 watch frequency

The IMO specify that the distress channels should be watched 24 h per day. The system should be designed so that the watch function is not desensitized by noise or interference. It is essential therefore that all transmit channels assigned for use on the transmitting station are selected so that no intermodulation products are allowed to fall within the frequency bands of the watch channels.

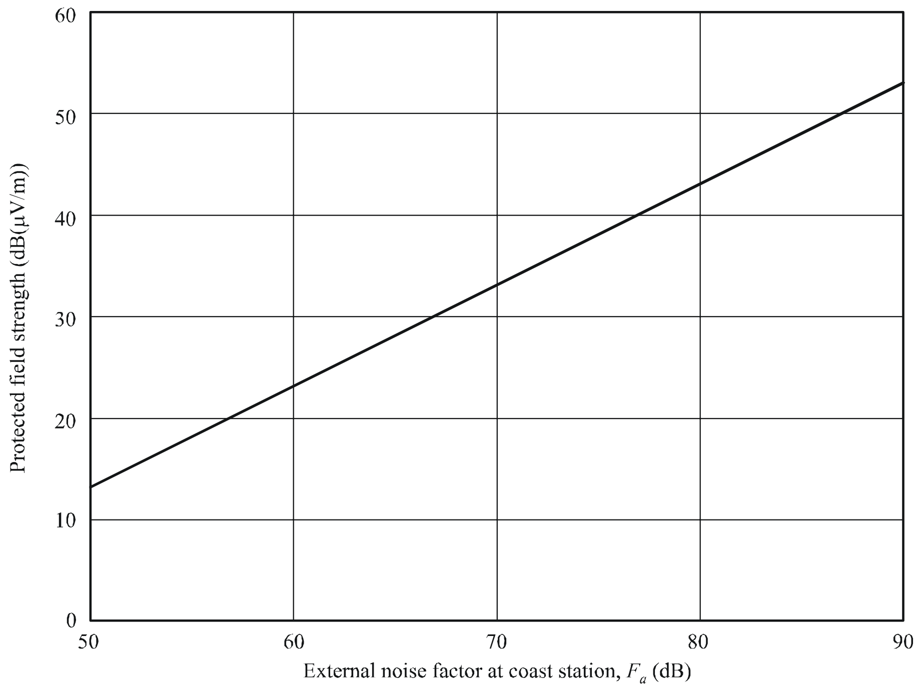
For very close channel separations the watch process can be threatened by energy in upper sideband of the adjacent SSB transmission falling within the receiver passband, where the wanted signal could be swamped by blocking or reciprocal mixing. Where channel separation is large enough to remove the threat of reciprocal mixing, a further, but lesser threat to the watch process may be sideband noise from the transmitter falling in the receiver passband.

The resulting DSC signal level reaching the shore station will depend upon the declared A2 range for the shore station, and in turn depend upon the sensitivity, F_a.

The level to be protected would be the level reaching the shore station after suffering a 3 dB fading loss, and is shown in Fig. 6.

FIGURE 6

Protected DSC field strength at receive site



1467-06

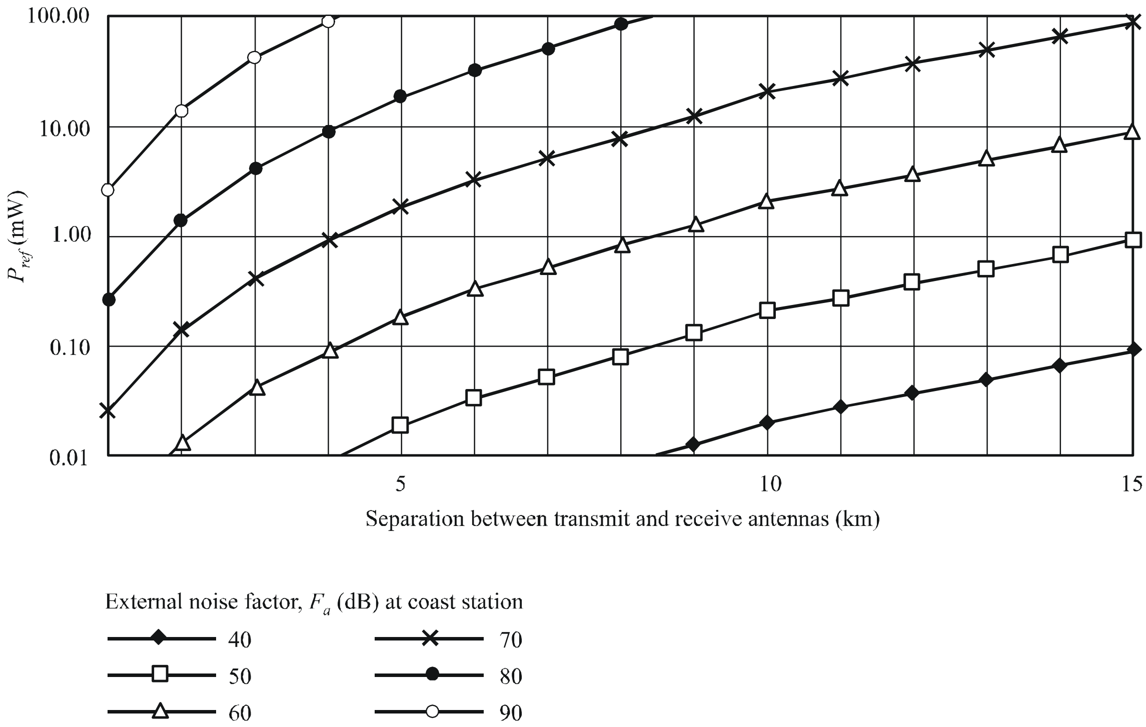
3.1 Impact of site separation on system performance

3.2 Estimating the level of the interference field

The tolerable amount of sideband noise leaving the transmit antenna, and the level of adjacent channel isolation required by the watch receiver both depend upon the separation between the transmit and receive antenna, and Fig. 7 provides a reference power P_{ref} (mW), which corresponds to the radiated power which would produce a field strength at the receive antenna equal to the DSC field strength to be protected and Fig. 8 provides a rule of thumb to relate this to transmitter and receiver characteristics.

FIGURE 7

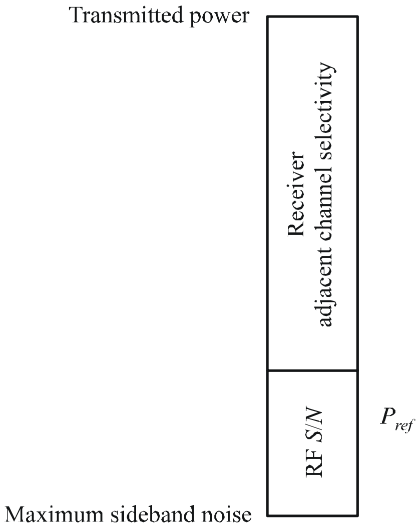
A2 Tx power yielding field strength equal to protected DSC field strength at receive site



1467-07

FIGURE 8

Relationship between transmitter and receiver characteristics



1467-08

3.3 Required adjacent channel selectivity

The level of adjacent channel isolation required by the watch receiver depends upon the separation between transmit and receive antennas. Figure 7 provides a reference power, P_{ref}, which corresponds to the radiated power which would produce a field strength at the receive antenna equal to the DSC field strength to be protected. If the receiver has an adjacent channel isolation figure of I_{adj} (dB), then the maximum power radiated by the station should be limited to:

$$P_{rad} = P_{ref} + I_{adj} \tag{5}$$

Three grades of receiver may be considered for providing the DSC watch: commercial communications receivers, ships' DSC watch receivers, or high performance crystallized DSC watch receivers, conforming with Table 6:

TABLE 6

Selectivity (dB)	**Offset (Hz)**
6	Between 150 and 220
30	Less than 270
60	Below 400
80	Less than 550

3.4 Protection from adjacent channel interference

The maximum permitted transmitter power should be determined using equation (6):

$$P_{Tx} = 30 + 10\log(P_{ref}) + I_{adj} - 10\log(Eff_{ant}) \tag{6}$$

where:

P_{Tx}: transmitter power (dBW)

I_{adj}: adjacent channel isolation figure for the receiver

Eff_{ant}: antenna efficiency.

For example, consider a receiver of the grade used on board ship having a typical adjacent channel isolation figure of 60 dB, on a site offering an F_a of 65 dB located 2.5 km from a transmit antenna with an efficiency of 75%. Figure 7 gives a P_{ref} of 0.1 mW and so the maximum level of radiated power would be 60 dB above 0.1 mW, which is 100 W. Allowing for antenna efficiency the maximum transmitter power would be 133 W. In order to benefit from a 500 W transmitter a pre-filter offering an additional 4 dB adjacent channel isolation would be required.

3.5 Protection from transmitter sideband noise

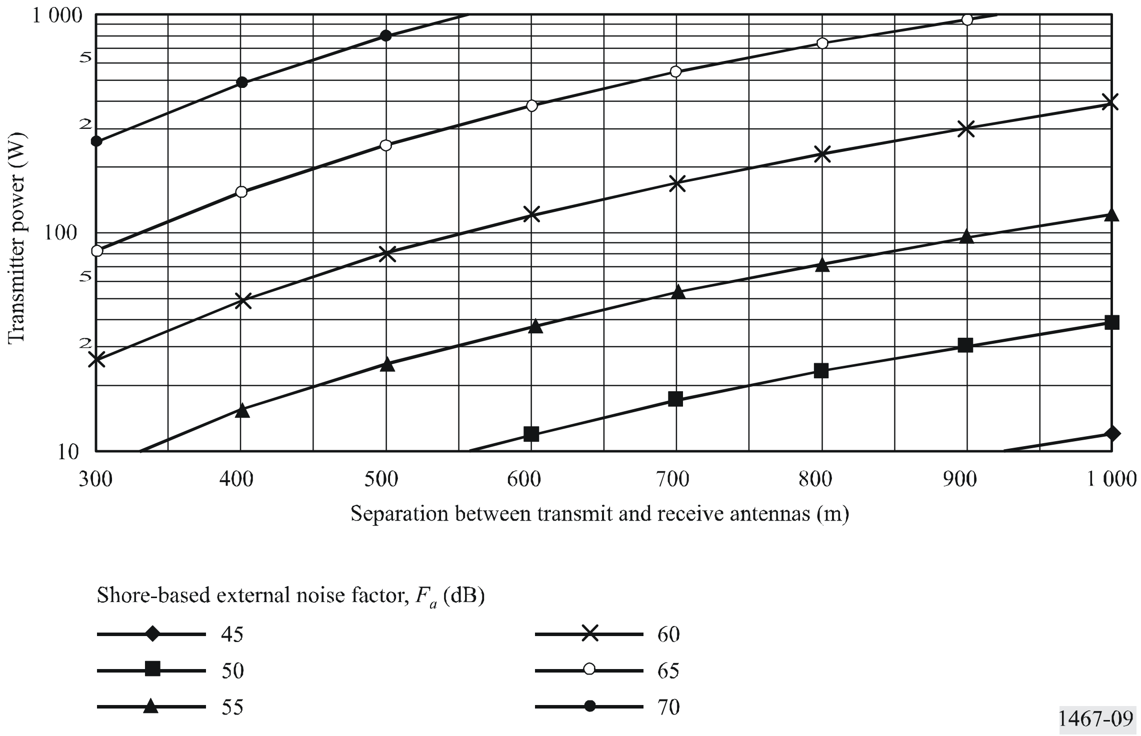
The maximum tolerable level of sideband noise is determined by the required C/N at the receive antenna. In the above example, for a S/N of 10 dB, the maximum tolerable level of sideband power would be 10 mW, which is quite low, and may call for use of a post-selector to reduce the noise leaving the transmitter modulator unit.

3.6 Co-site operation

Figure 9 shows the effect of reducing the separation between the transmit and receive antenna below 1 km to 300 m, the minimum value computed using GRWAVE. By way of example, if a station close to the shoreline had a maximum annual median external noise factor F_a of 65 dB then from Fig. 4 the range achieved would be just over 200 nautical miles. If the adjacent channel isolation were 80 dB, then for an e.m.r.p. of 200 W the antenna separation should be not less than 450 m.

FIGURE 9

Transmitter power versus antenna separation for 80 dB adjacent channel isolation



Under such circumstances a long feeder would be required to attain the separation required. As the frequency increases there is a considerable reduction in external noise and increase in feeder loss. At 2 MHz the external noise factor is very much greater than the system noise factor, and for a system noise factor of 15 dB up to 10 dB of feeder loss would be tolerable on a well designed and maintained system. A cost-effective way to avoid the cost of a very long low loss coaxial cable would be to use a separate antenna for A2.

4 Software requirements

4.1 Noise calculation

To simplify the determination of range for A2 and NAVTEX transmissions a modified form of NOISEDAT is ideally required including calculation of F_{am} in accordance with the procedures of this Recommendation.

4.2 Intermodulation

In order to protect the DSC watch channels from the harmful effects of interference caused by intermodulation products, a new program is ideally required to enable the frequencies assigned for use on a shore-based transmitting station to be checked to ensure that no intermodulation products are produced within the passbands of the DSC watch receivers, down to at least the 9th order. Such software should account for the offset spectrum occupied by SSB transmissions to be used.

RECOMMENDATION ITU-R M.1637

Global cross-border circulation of radiocommunication equipment in emergency and disaster relief situations

(2003)

The ITU Radiocommunication Assembly,

considering

a) that public protection radiocommunication is radiocommunication used by responsible agencies and organizations dealing with maintenance of law and order, protection of life and property, and emergency situations;

b) that disaster relief radiocommunication is radiocommunication used by agencies and organizations dealing with a serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as the result of complex, long-term processes;

c) that disaster relief operations have evolved over the years to make use of radiocommunication systems as a reliable and effective means of communication for the crucial success of the disaster relief operation;

d) that many international disaster relief organizations utilize telecommunication networks for coordinating their efforts and for linking to authorities and affected persons when providing emergency care;

e) that providers of international humanitarian assistance employ and depend on non-dedicated radiocommunication equipment which is widely in use and available, including amateur radio and mobile portable satellite facilities for their telecommunications during international disaster relief operations;

f) that disaster relief users have operational requirements that may differ from other wireless users;

g) that the importation and circulation of radiocommunication equipment is usually required when the local telecommunication infrastructure is damaged, overloaded or non-existent in the area of the disaster;

h) that when an emergency or disaster occurs, the speed of the response is critical;

j) that the efforts of emergency and disaster relief workers are often delayed by a number of factors which may include actions by some administrations that:

– restrict or prohibit the import and use of radiocommunication equipment;
– have lengthy and/or costly immigration and customs procedures;
– lack an expedient process for the authorization to operate radiocommunication equipment or for the permission to use radiocommunication equipment in border areas;
– insist on the use of certain types of fixed frequency radios making it technically difficult to operate in changing situations,

noting

a) that national and regional authorities should, when possible, and in conformity with their national laws, cooperate in order to reduce and remove any obstacles hindering global cross-border circulation of radiocommunication equipment intended for use in emergency and disaster relief situations, particularly to:

– develop agreements and regulations intended for use in emergency and disaster relief situations from all import, export and transit duties,

recognizing

a) that Resolution 645 (WRC-2000) invites ITU-R to conduct studies for development of a Resolution concerning the technical and operational bases for global cross-border circulation of radiocommunication equipment in emergency and disaster relief situations;

b) that the World Customs Organization (WCO) has developed two international agreements which are applicable to radiocommunication equipment intended for disaster relief operations:

– the *Istanbul Convention*, which binds countries to eliminating customs duties on personal effects and professional equipment carried by visitors;

– the *Professional Equipment Convention*, which has so far been adopted by about 40 countries, which exempts from customs duties equipment used by professionals, e.g. journalists, doctors, relief workers, businessmen, etc.;

c) that the United Nations Office for the Coordination of Humanitarian Affairs (UN-OCHA) which has the mandate to coordinate international humanitarian assistance, disaster relief and disaster mitigation convenes the Working Group on Emergency Telecommunications (WGET), an inter-agency forum of entities concerned with humanitarian assistance;

d) that WGET is following up on potential applications of Resolution 645 (WRC-2000) to deal with regulatory issues, specifically regarding the trans-border use of telecommunication equipment during acute emergencies;

e) that the Istanbul Declaration of WTDC-02 included among a number of pressing issues, the importance of emergency telecommunications;

f) that the 1998 Intergovernmental Conference on Emergency Telecommunications (ICET-98), with the participation of 76 countries and various intergovernmental and non-governmental organizations, adopted the Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations. In 1998, 33 States signed this comprehensive Convention which also contains an article dealing with the removal of regulatory barriers. Thirty ratifications or definitive signatures are needed by June 2003 for entry in force;

g) that the World Radiocommunication Conference (Istanbul, 2000), has revisited Resolution 644 (Rev.WRC-2000) which:

– urges administrations to take all practical steps to facilitate the rapid deployment and effective use of telecommunication resources for disaster mitigation and disaster relief operations by reducing and where possible removing regulatory barriers and strengthening trans-border cooperation between States;

– invites the ITU-R to continue to study, as a matter of urgency, those aspects of radio-communications that are relevant to disaster mitigation and relief operations;

h) that the Information Technology Agreement (ITA) of the World Trade Organization (WTO) aims at eliminating import duties on all information technology equipment including wireless terminals and equipment;

j) that administrative arrangements for circulation should be aimed at simplifying existing regulation;

k) that inter-administration measures facilitating cross-border use of radio equipment exist in some cases,

recommends

1 that, when discussing circulation of any radiocommunication equipment for emergency and disaster relief situations, present needs as well as future and advanced solutions should be taken into account;

2 that, in order to facilitate a speedy authorization process for the operation of radiocommunication equipment in emergency and disaster relief situations, the regulatory authorities are encouraged to develop plans and rules in place before a possible disaster that:

– facilitate the operation of radiocommunication equipment by visiting personnel in the territory of the disaster/emergency;

– facilitate the use of radiocommunication equipment that such organizations employ;

– take into account, as appropriate, the frequencies of the radiocommunication equipment that will be used by such organizations;

3 that, in order to establish the technical basis for global circulation of radiocommunication equipment in emergency and disaster relief situations, such equipment needs to fulfill the requirement for avoiding harmful interference in any country where they circulate:

– by conforming to ITU-R Recommendations, particularly with regard to emission limits.

RECOMMENDATION ITU-R M.1746

Harmonized frequency channel plans for the protection of property using data communication

(2006)

Scope

This Recommendation addresses system interoperability and harmonized frequency channel plans for the protection of property using data communication.

The ITU Radiocommunication Assembly,

considering

a) that technologies exist and are being developed which facilitate, through public protection radiocommunication systems, the protection of property;

b) that the usefulness of public protection radiocommunication systems for the protection of property have been and continue to be demonstrated using data transmissions;

c) that many administrations wish to promote interoperability and interworking between systems used for public protection both nationally and for cross-border operations;

d) that national spectrum planning for public protection radiocommunication systems need to have regard for cooperation and bilateral consultation with other concerned administrations, in order to facilitate greater levels of spectrum harmonization;

e) that current public protection systems mostly require relatively low communications bandwidth, and may use either narrow-band communication systems supporting voice and low data-rate applications, typically in channel bandwidths of 25 kHz or less, or spread spectrum technology;

f) that to facilitate system interoperability and/or interworking, it is desirable that systems for the protection of property be developed under an open architecture without releasing sufficient information to allow systems to be easily countered;

g) that a description of such frequency use and radiocommunication systems providing protection of property is given in Annex 1;

h) that usage of the same frequencies of the same allocation in particular ITU regions will enable administrations to benefit from harmonization while continuing to meet national planning requirements;

j) that use of common frequencies within which radiocommunication equipment for the protection of property can operate, compatible technology, mutual cooperation and consultation will ease the radiocommunication system interoperability and/or interworking of protection of property systems, *recognizing*

a) that a common frequency or a common frequency band may be available within each country;

b) that countries use a variety of frequency bands, technologies and applications for the protection of property;

c) that several countries have implemented or are considering implementing protection of property systems,

noting

a) that many administrations use the same frequencies for narrow-band protection of property applications;

b) that such applications on these frequencies can provide good signal availability over large coverage areas;

c) that it is desirable to identify frequencies on a regional basis, which will permit spectrum channel harmonization for the protection of property;

d) that these property protection applications are achieved through data transmissions;

e) that data transmissions on harmonized spectrum will facilitate interoperability only with compatible technology;

f) that Report ITU-R M.2033 encourages public protection agencies and organizations to utilize relevant ITU-R Recommendations in planning spectrum use and implementing technology and systems supporting public protection;

g) that Report ITU-R M.2033 also details the public protection agencies' and organizations' user requirements, including system requirements, security and cost;

h) that ITU is emphasizing the need for ITU-R efforts on telecommunications for public protection,

recommends

1 that administrations should cooperate with other administrations in their region to achieve harmonized frequency channel plans for protection of property systems and/or applications (such as stolen vehicle recovery). Appendix 1 presents some frequency channel plans for the protection of property using data communications;

2 that techniques for ensuring interoperability of different systems should also be taken into account.

Annex 1

Description of systems providing protection of property

1 Introduction

This Annex provides a description of systems which provide for the recovery of stolen or missing property, and which thereby act as a deterrent against theft or tampering. It provides a functional description of such systems, as well as functional characteristics. It also includes a description of the systems' radiocommunication parameters.

2 General system description

Property protection systems require communications between a centralized, typically fixed control network, and many remote transceivers located with or within assets being protected. The control network is responsible for allocating and controlling transceiver identifiers, and may poll the transceivers either regularly, or on demand, specifically when an asset is reported as having been stolen. The control network may be operated by national authorities or responsible agencies and organizations, and in either case may have arrangements for cooperation with other property protection systems operating within the same or different countries. The transceiver may be configured to only respond to messages received from the control network, or initiate communications when it detects tampering or theft, or a combination of these. Systems use a variety of communications, including fixed and mobile radio communications and private circuit and public telecommunications, depending on configuration and the mobility of the protected items. Transceivers may be configured to provide location information in their transmissions (e.g., derived from a satellite navigation system), or systems may rely on triangulation or searches using mobile control units. The communications for property protection are often configured to provide high levels of coverage in traditionally difficult to reach locations such as underground garages and metallic shipping containers to which stolen items may be taken for concealment or modification.

3 System function

How the different systems function depends on the system architecture.

The control centre maintains a database of asset information comprising transceiver configuration and unique system identifiers, information on who may receive reports or instigate activity, and procedures to be followed when an alert is raised. Communications within the property protection network and between the network and transceivers attached to the protected assets are automated and under computer control, though may be instigated manually, for example following a report of an asset being stolen.

In systems which rely on the control centre to initiate or control transceiver activity (either configuration commands or requesting status responses), the communication may be either made directly through telephone lines for fixed assets, or through a network of many radio transmitters for either fixed or mobile assets. In other systems, the transceiver located with or within the asset being protected may initiate communications if it detects that tampering or theft is taking place. The communication may once again be direct through the public telephone network, or by radio to one or more receiver sites configured to receive property protection messages and relay information back to the control centre. However the messages are instigated or communicated, the control centre will maintain a record, and as appropriate, involve or inform other organizations.

Radiocommunications may be used between the control centre and any remote transmitters and receivers belonging to the control network, in addition to those between the transceiver and the control network. Any such transmissions within the control network would resemble normal telemetry and are not covered by this Recommendation, which concentrates on the communication between the control network and the protected device. These communications may be arranged in a variety of ways such that the transceiver responds on the same channel on which it receives commands, an adjacent channel, or using an entirely different channel or technology, for example receiving commands on a dedicated property protection channel and responding either through a call on a cellular telephone network, or using a shared, short-range channel to receivers located with cellular base stations with which back-haul infrastructure is shared. It is normal for transceiver transmit power to be low, in order to minimize power drain and possible interference if the asset is taken outside of the coverage area of its own network, and this may encourage the use of different bands and technologies for the receive and transmit segments.

If assets may be moved across national boundaries, cooperation arrangements with property protection network operators in other countries are advantageous, as are commonly agreed or harmonized allocations and assignments. The situation can be further improved by having transceivers listen for messages on several channels, and possibly accept commands with configuration instructions on which channel or technology to use for responses.

Depending on the size and cost of the assets being protected, some transceivers may include location information (possibly derived from satellite navigation systems) in their transmissions, while other networks may rely on localization through the received signal, either by triangulation or “homing” with mobile receivers.

While the main use of property protection systems is expected to be for recovery of valuable, mobile items (vehicles, boats) following theft, property protection systems may also be used to monitor and report tampering in remote equipment (vending machines), track delivery vehicles to enhance security or provide better, up-to-date information on delivery schedules, or provide fall-back alert cover for emergency teams or shipments of money or other valuables. Each of these applications makes different demands on the property protection network, transceivers and communications, however a mixture can improve overall network utilization.

4 Radiocommunication characteristics

These systems often interface with the public switched telephone network, paging or public cellular networks, and with other radiocommunication equipment at remote device locations. They typically operate in a frequency range from HF and up to about 1 GHz depending upon the technology used, but many systems are operated in fixed and mobile service allocations in the range 100-900 MHz.

5 Interoperability

Through the use of systems as described above, operating on the same frequency and using compatible system devices, the property which is being protected through recovery can be easily located if the property is in another country different from the one in which it was taken. Harmonization of frequencies for this type of application is particularly useful for interoperability between countries and to ease the burden of coordination for administrations. Presently in Region 1 such systems use 25 kHz or 12.5 kHz channels, or broader channels if spread spectrum technologies are employed. In certain countries of Region 2 and in Region 3 a 25 kHz channel is used to provide these services.

Appendix 1

Frequency channel plans for the protection of property using data communications

The frequencies below have already been assigned or are being considered for assignment for protection of property radiocommunication systems:

In Region 1

Europe: Frequencies within the harmonized band 169.4-169.8125 MHz[1]

Frequencies presently used in other bands including 138.625 MHz, 138.650 MHz, 149.025 MHz, 162.050 MHz and 164.175 MHz on a national or multinational basis with agreement between administrations

Arab States: No frequency has been agreed upon yet

Africa: One channel centred at 169.200 MHz in two countries.

In Region 2

CITEL has recommended frequencies within the range 173.0-173.3 MHz.

In Region 3

One channel centred at 163.475 MHz in some countries.

---

[1] In Europe, CEPT/ECC Decision (05)02 of 18 March 2005 *"on the use of the frequency band 169.4-169.8125 MHz"* has been adopted, with provisions for both high and low power harmonized channels for asset tracking systems. An appropriate transition period may be required for existing systems in use on other frequencies which intend in the future to use those in the CEPT/ECC Decision.

RECOMMENDATION ITU-R BT.1774*

Use of satellite and terrestrial broadcast infrastructures for public warning, disaster mitigation and relief

(Question ITU-R 118/6)

(2006)

Scope

This Recommendation provides characteristics of satellite and terrestrial broadcasting systems used for disaster mitigation and relief operations. Detailed descriptions of these systems are also given in Annex 1 as guidance.

The ITU Radiocommunication Assembly,

considering

a) the recent natural tragedies due for example, to earthquakes and their consequences, alongside the possible role of communications in public warning, disaster mitigation and relief;

b) that all administrations recognize the need to organize information dealing with public warning, disaster mitigation and relief;

c) that in cases, when the “wired” or “wireless” telecommunication infrastructure is significantly or completely destroyed by a disaster, broadcasting services can often still be employed for public warning, disaster mitigation and relief operation;

d) that broadcast frequency bands are largely globally harmonized and could be used for disseminating public alert messages and advice to large sections of the population;

e) that broadcast frequency bands could be used for coordination of relief activities by disseminating information from relief planning teams to the population and provide information on the well-being of individuals, especially from the affected area;

f) that within the terrestrial broadcasting infrastructure there are a number of systems offering communication services that allow global or regional coverage;

g) that users of the broadcasting services are expected to be using both portable and fixed terminals for emergency services, especially in sparsely populated, uninhabited or remote areas;

h) that within the broadcasting services there is a great and growing need to determine standard international routing procedures for emergency traffic;

j) that many administrations have already established emergency communication traffic procedures including means for secure control of their utilization;

k) that distress, emergency, safety and other communications are defined in the Radio Regulations (RR);

l) that individual broadcasters will always have their own security control over their programme material and their network;

* This Recommendation should be brought to the attention of Telecommunication Standardization Study Groups 9 and 16 and Telecommunication Development Study Group 2.

m) that many stations operating in the broadcasting service can operate without externally provided power for some time (up to weeks);

n) that sound and television broadcasting organisations have developed techniques often referred to as “electronic news gathering” for the dissemination of information in programmes called “news bulletins” to inform the public of the extent of disasters and the recovery efforts being undertaken,

recognizing

a) that the broadcasting infrastructure is actually used to reach several billion people in a short period of time;

b) that in some countries, such alert systems such as the emergency warning system (EWS) or emergency alert broadcasting have been implemented in which broadcasting stations are connected to governmental or international organizations which issue disaster forecasts;

c) that a single transmitter operating in the LF, MF and HF frequency bands as well as space stations of the BSS cover large service areas;

d) that the RR foresee provisions by means of which BSS feeder links subject to Appendix 30A can be converted into FSS links (e.g. for VSAT operations in an emergency area);

e) that in some cases, a broadcasting station has its own seismometers in the country, analyses the seismic intensities, and voluntarily issues precautions to the public through broadcasts;

f) that ITU-R has established studies into spectrum usage and users requirements for terrestrial electronic news gathering in Radiocommunication Study Group 6,

recommends

1 that responsible agencies should prepare procedures and routines to send information on public warning, disaster mitigation and relief to transmitting or network distribution centres in accordance with agreed technical signal protocols;

2 that broadcast transmitters and receivers should be equipped to receive material prepared by the responsible agencies;

3 that systems for transmission and reception should include the possibility for forcing suitably equipped and suitably primed receivers (whether switched on or in standby mode) to present programme material for disaster mitigation and relief without intervention from the listener or viewer; so that all citizens can become informed of a possible disaster within the shortest possible period of time; with a robust mechanism against abuse of this feature;

4 that for *recommends* 1-3, public warning systems on broadcasting as given in Annex 1 should be considered;

5 that in case of public warning, disaster mitigation and relief, broadcasting transmitters should disseminate information advising at a local, national level and/or, potentially, even across national borders as appropriate;

6 that administrations should coordinate where possible with sound and television broadcasting organizations the application of electronic news gathering resources in the disaster area to maximize the potential for using the information gathered in a timely and coordinated fashion to assist the disaster mitigation and relief efforts.

Annex 1

Public warning systems on broadcasting

1 Introduction

This Annex presents an overview of public warning systems in the broadcasting service.

2 Outline of public warning systems on broadcasting

Broadcasters have two functions in disaster management. One is gathering or receiving information from disaster radiocommunication networks connected to administrative organizations. The exclusive line connected to the administrative organizations is preferably to be used for urgent alerts and such information as earthquake and tsunami data. The other function is delivering information to the general public. Some municipalities in some countries may have a multicasting system to outdoor receivers with loudspeakers in their own disaster radiocommunication network. However, it may be difficult to hear the sound indoors, especially in bad weather such as storms or heavy rain. Therefore, disaster alerts and information via broadcasting is useful for disaster mitigation.

3 EWS for analogue broadcasting

The system should use relatively simple equipment and ensure stable operations. In an emergency, the EWS control signal, which is an analogue signal, replaces the programme signal (radio and TV sound), automatically activating the receivers equipped with EWS function even when they are sleeping.

The EWS control signal can be used for alarm sound to draw the attention of listeners/viewers to emergency broadcasting programmes. Broadcasters operating TV and radio can transmit the EWS control signal. The EWS control signal includes an area code as well as a time code, keeping the receiver protected from intentional fake control signals.

4 EWS for digital broadcasting

In digital broadcasting, the EWS control signal is transmitted by multiplexing with broadcast wave. It automatically activates the receivers equipped with the EWS function when they are sleeping. The EWS control signal should be robust against the abuse of this feature. It is foreseen that the receiving function of digital broadcasting will be installed in mobile terminals such as cellular phones. It is effective to send emergency information to such mobile terminals. Therefore, such mobile terminals are desired to be equipped with the EWS function for digital broadcasting.

Appendix 1

Examples of public warning systems on broadcasting

1 Introduction

This Appendix presents a system overview and the current status of public warning systems on broadcasting in some countries/regions.

2 Japan

This section describes the present state of public warning systems on broadcasting in Japan. This system is called the emergency warning system (EWS).

2.1 Disaster management system

This section provides some information on the disaster management system in Japan for the public warning system on broadcasting.

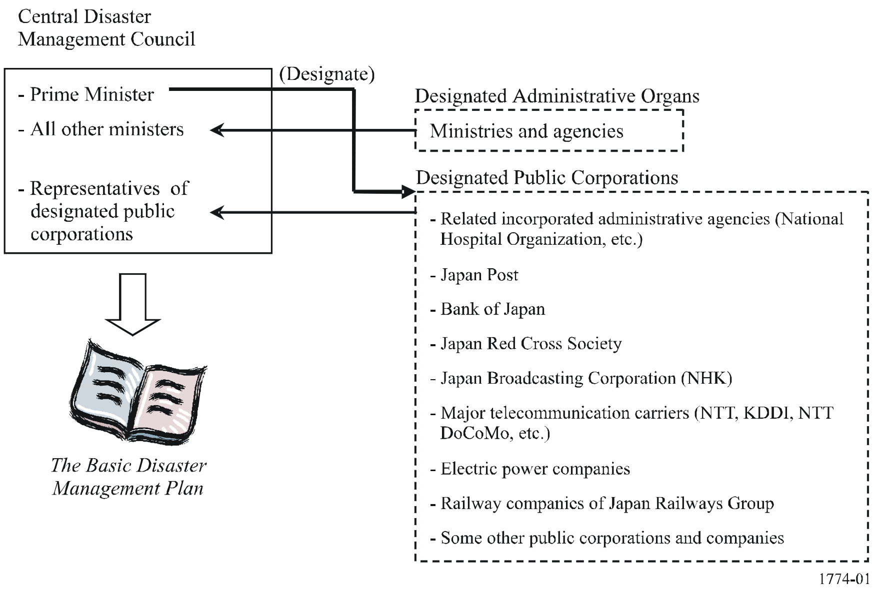
2.1.1 Disaster management plans

The disaster management system is specified in the disaster countermeasures basic act. The prime minister designated Japan broadcasting corporation (NHK) as the designated public corporation and the governor of each prefecture designated most commercial broadcasters operating terrestrial broadcasting stations as designated local public corporations.

On the national level, the Central Disaster Management Council is organized with the representatives of designated public corporations. The Council formulates the basic disaster management plan as the national master plan, and promotes execution of the plan (Fig. 1):

FIGURE 1

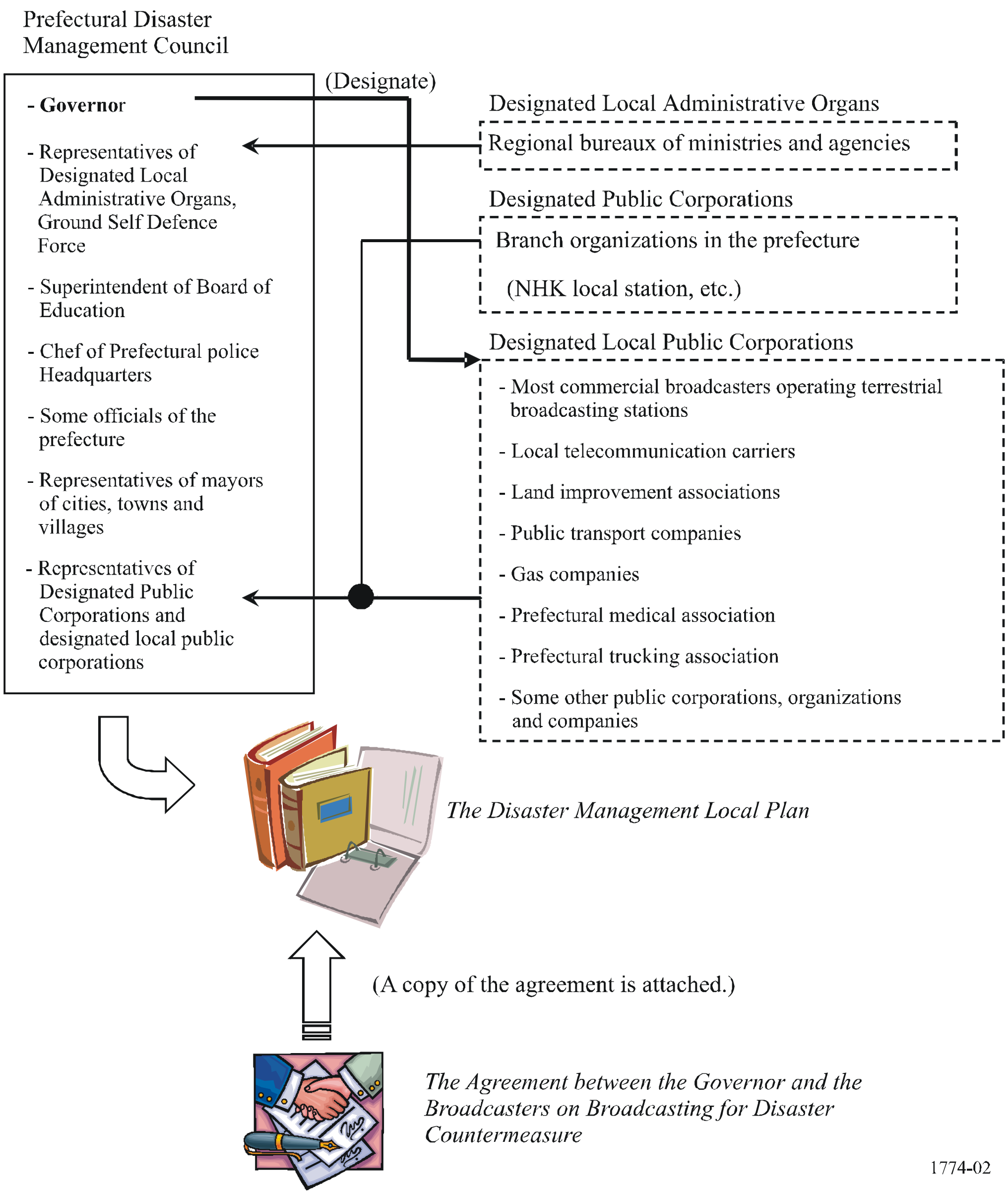
The structure of disaster management (national level)



On the prefectural level, the Prefectural Disaster Management Council is organized with the representatives of designated public corporations and designated local public corporations. The Council formulates the disaster management local plan, and promotes execution of the Plan (Fig. 2).

FIGURE 2

The structure of disaster management (prefectural level)



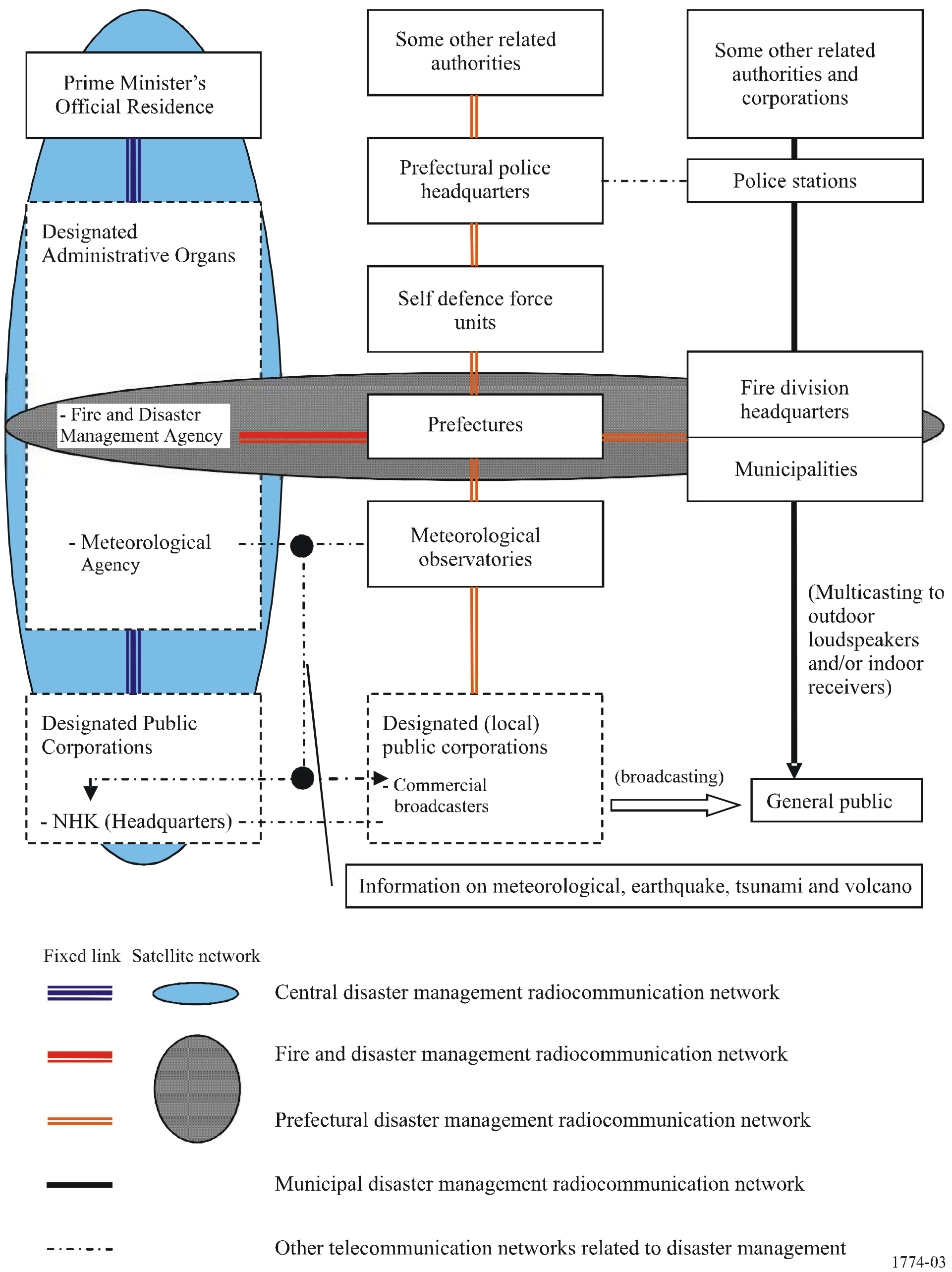
The disaster management local plan consists of several volumes, such as "Earthquake disaster countermeasures", "Storm and flood countermeasures", "Volcano disaster countermeasures". The Plan is also used as the manual of disaster management. Therefore, the copy of the agreement between the governor and the broadcasters on broadcasting for disaster countermeasures is attached to the Plan. The procedure for broadcast request by the governor or the mayors to the broadcasters is specified by the agreement and would be reflected to the Plan.

2.1.2 Telecommunication networks for disaster management

In the case of an emergency, the traffic of public switched telephone networks would be increased and it would be difficult to connect to the destinations. Wired telecommunication lines would suffer from some disasters. Therefore, it is very important to ensure an independent radiocommunication network for disaster management. Figure 3 shows disaster radiocommunication networks and related telecommunication networks in Japan. Disaster radiocommunication networks are established in the three layers of national, prefectural and municipal.

FIGURE 3

Disaster management radiocommunication and related network



Broadcasters have two functions in the networks. One of them is gathering information. For this purpose, disaster radiocommunication networks connected to administrative organs are used. In addition, the exclusive line from the meteorological agency is also used for urgent alert and such information as earthquake and tsunami data.

The other function is delivering information to the general public. Many municipalities have a multicasting system to outdoor receivers with loudspeakers in their own disaster radiocommunication network. However, it is difficult to hear the sound indoors, especially in bad weather such as storms or heavy rain. Though a few municipalities lend indoor receivers to its residents, it is expensive. Therefore, disaster alert and information via broadcasting is also useful for disaster mitigation.

2.1.3 Disaster management drills

Disaster management drills are conducted in order to confirm and verify that the disaster management system of each organization is capable of smoothly carrying out the required activities should a disaster occur. On 1 September, disaster management day (the day in 1923, Great Kanto Earthquake occurred), the government and related disaster management organizations mutually cooperate to hold wide-ranging, large-scale disaster management drills throughout Japan. Additionally, in each region, drills based on past disasters are conducted year-round.

Broadcasters participate in the training activities of these national and regional disaster management drills in addition to the training within each organization.

2.2 Earthquake and tsunami warning broadcasting

2.2.1 Gathering information

2.2.1.1 Japan meteorological agency’s quick reports on earthquake and tsunami

Japan, an archipelago that lies on several active seismic faults, has experienced numerous earthquakes in the past that have left many people dead. The 1993 earthquake off the south-western part of Hokkaido created a massive tsunami that struck the island of Okushiri in just 5 min, killing 202 people and leaving 28 people missing, and severely damaging property. It was after this incident that the Meteorological Agency began studying a system to quickly issue a tsunami warning in the event of an earthquake.

In March 1995, the agency launched a system capable of the following:

– About 2 min after an earthquake, issuing emergency quake intensity (quake intensity of a particular zone viewed as a two-dimensional plane, with the entire country divided into about 150 zones (currently 180)).

– About 3 min after the quake, issuing a tsunami warning.

– About 5 min after the quake, issuing individual quake intensity (at about 3 700 points across the country where seismographs are installed, including those managed by municipalities).

Under this system, the agency increases the number of seismographs to improve the accuracy of quake intensity measurement and tsunami warnings. First, the emergency quake intensity gives preliminary information about the earthquake, enabling the agency to quickly assess whether a tsunami warning should be issued or not. Next, the individual quake intensity is issued.

The new system is thus designed primarily to speed up the process of issuing a tsunami warning. Furthermore, as the tsunami danger area is divided into 66 zones, the agency can issue a tsunami warning with greater accuracy. In addition to its domestic quake observation network that crisscrossed the country, the agency uses information provided by the incorporated research institutions for seismology (IRIS) and the pacific tsunami warning center (PTWC) in Hawaii to issue a tsunami warning in the event of an earthquake in the seabed of the pacific ocean.

2.2.1.2 Broadcaster’s own network of seismographs

The seismic data from the Meteorological Agency reaches NHK about 2 min after an earthquake. Other than this seismic observation network operated by the agency, NHK has its own seismographs installed at 72 points across the country, from which it gathers seismic data about 20 s to 1 min after an earthquake. With this data, NHK can immediately prepare to broadcast the seismic data from the agency upon arrival. If the quake intensity is estimated to exceed the danger level, NHK begins broadcasting seismic information ahead of the agency. The commercial broadcasters also measure seismic intensity data and use its emergency broadcasting operation as well as NHK.

2.2.1.3 Robot cameras

NHK has about 440 robot cameras stationed across the country. Those installed along coastlines are the first to warn the public of the most imminent tsunami danger. Although of low image quality, the pictures recorded by these 440 robot cameras are stored for 12 h in a robot camera monitoring system. The system automatically picks robot cameras of the most affected areas, and displays the images at the moment when the quake occurred. With these automatically produced quake/tsunami information images, robot cameras, and monitoring system, NHK is the first to provide accurate information on earthquakes and tsunami immediately after they occur.

The commercial broadcasters also set robot cameras and use them in a breaking report of the earthquake as well as NHK.

2.2.2 Delivery information

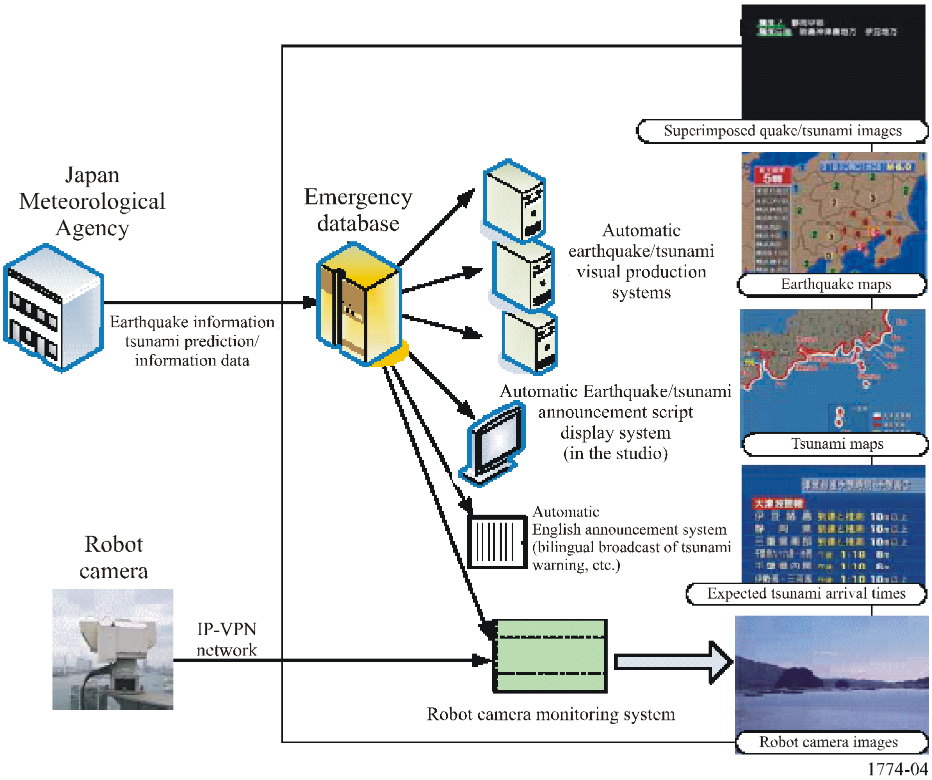
2.2.2.1 Earthquake and tsunami warning broadcasting system

The Meteorological Agency had modified and upgraded its earthquake and tsunami warning system from 1995 till 1999, and NHK followed by renewing its tsunami warning broadcasting system. Earthquake and tsunami data issued by the agency are first transmitted to NHK over data lines. At NHK, its computers will then automatically produce a variety of visual information including “superimposed quake/tsunami images”, “earthquake maps”, “tsunami maps”, and “expected tsunami arrival times”. Scripts to be read by an announcer on air will also be automatically produced by an announcement script display system based on data provided by the agency. Upon receiving seismic data from the agency, NHK will immediately begin broadcasting quake/tsunami programmes with the latest information (Fig. 4).

The commercial broadcasters also construct the system that can promptly broadcast latest information on the earthquake and the tidal wave as well as NHK.

FIGURE 4

The earthquake and tsunami warning broadcasting system



2.2.2.2 Emergency console

In 1992, the NHK News Centre installed an "emergency console" (Fig. 5) to further speed up the broadcasting of earthquakes and other emergency news programmes. This console makes it far simpler and quicker to make changes in prearranged programmes as such changes are necessary to broadcast emergency news.

FIGURE 5

Emergency console

If a tsunami warning is issued, NHK will broadcast an emergency warning to warn the public of possible dangers. The moment it receives a tsunami warning from the Meteorological Agency, NHK uses the console to complete preparations for emergency broadcasting through all of its 13 media (terrestrial television, radio, satellite broadcasting) outlets. Upon pressing only one button of the console, emergency news programmes will be aired automatically.

2.3 EWS over analogue broadcasting

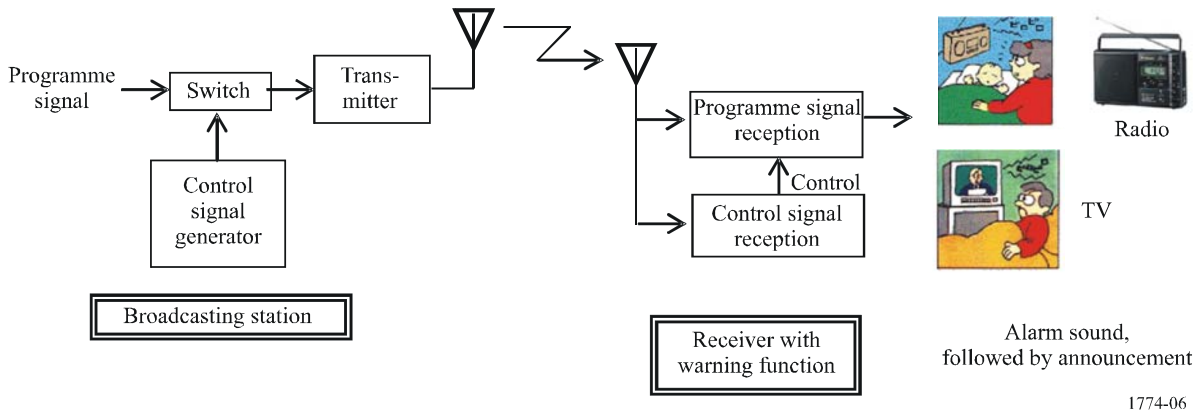
2.3.1 Overview

The emergency warning system developed by NHK Science and Technical Research Laboratories (NHK STRL) in the 1980s, promptly and effectively conveys to the public emergency notices such as tsunami warnings. It works through conventional broadcasting systems by automatically actuating warning receivers. This service has been in operation since 1985 in Japan.

The composition of a typical emergency warning system is shown in Fig. 6. In an emergency, the control signal replaces the programme signal (radio and TV sound), automatically activating the warning receivers even when they are switched off. The control signal is composed of two frequencies near 1 kHz and set at a level higher than the normal programme signal. The control signal is also used for the warning sound. The system uses relatively simple equipment to ensure stable operations.

FIGURE 6

Composition of emergency warning system for analogue broadcastings



The warning receiver issues a special alarm sound, a demodulated control signal, to draw the attention of listeners/viewers to emergency broadcasting programmes. At NHK, the control signal can be transmitted through satellite TV, terrestrial TV, MF radio and FM radio. Many commercial broadcasters operating terrestrial TV and MF radio can also transmit the control signal. The control signal includes an area code as well as a time code, keeping the warning receiver shielded from intentional fake control signals.

In Japan, several types of warning receivers have been commercially produced. NHK and many commercial broadcasters periodically transmit test control signals in emergency warning broadcasting on the first day of each month.

2.3.2 Operation of EWS

Broadcasters operate EWS only in the following cases:

		Start signal	Area code
(1)	Large-scale earthquake warning statement is declared by Meteorological Agency	Category I	Nationwide
(2)	Including broadcasting of evacuation order is requested by governor of prefecture	Category I	Prefecture or wide area
(3)	Tsunami warning is declared by Meteorological Agency	Category II	Nationwide, prefecture or wide area

Category I activates all EWS receivers in the service area. Category II activates only the relevant EWS receivers.

In cases (1) and (2), broadcasters will transmit the Category I start signal. In case (3), as inland users do not need to evacuate, broadcasters will transmit the Category II start signal.

After the emergency warning message, broadcasters will transmit the end signal to turn off EWS receivers.

2.3.3 Specification and configuration of EWS signal

The modulation method of the EWS signal is the frequency shift keying (FSK) method with a space frequency of 640 Hz and a mark frequency of 1 024 Hz. The allowable frequency deviation is plus or minus ten parts per million in each case. The transmission speed of the EWS signal is at 64 bits per second and this deviation is ten parts per million. Signal distortion is below 5%. The configurations of the Category I start signal and Category II start signal are shown in Fig. 7, and that of the end signal is shown in Fig. 8.

FIGURE 7

The configurations of Category I start signal and Category II start signal

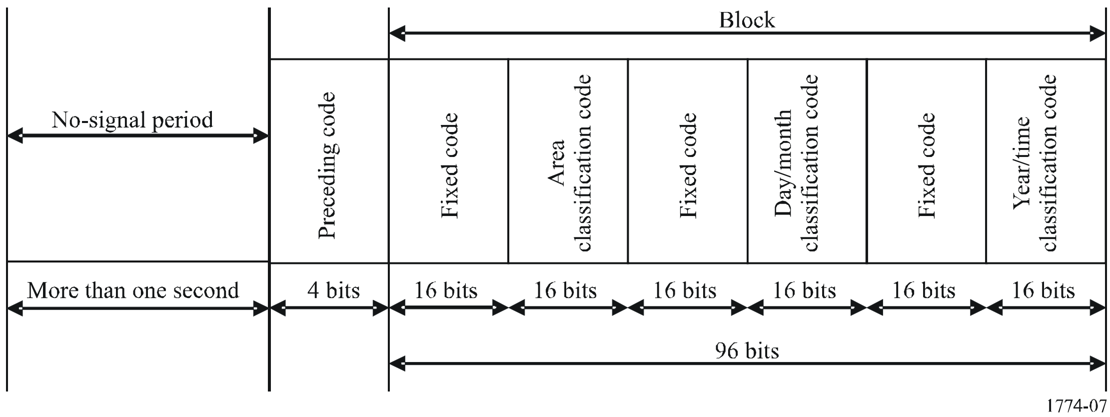
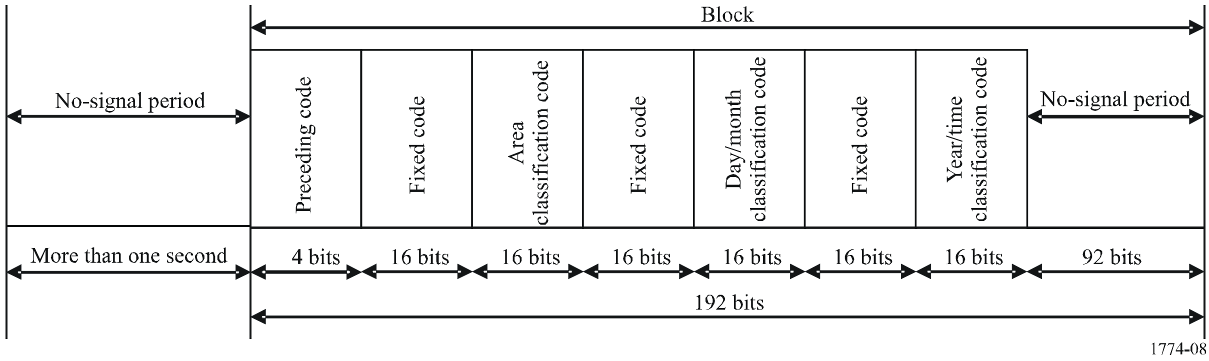


FIGURE 8

The configurations of end signal



Notes for Figs. 7 and 8:

1 *Fixed code:* The fixed code consists of a 16-bit code inherent in the EWS signal. It is used for extracting the EWS signals from sound signals. Furthermore, it is used for distinguishing between the Category I start signal and the Category II start signal.

2 *Area classification code:* The area classification code is for operating a receiver in restricted regional areas. The purpose of this code is to avoid triggering receivers other than the relevant receivers by anomalous propagation of broadcasts.

3 *Year/month/day/time classification code:* The year/month/day/time classification code is used for transmitting real-time information for preventing operation of receivers by illegal radiowaves that are recorded and retransmitted after the EWS signals have been transmitted.

2.4 Digital emergency warning system (digital EWS)

This section introduces details regarding the digital emergency warning system (digital EWS) using digital broadcasting.

In digital broadcasting, the EWS signal is transmitted by multiplexing with the broadcast wave the same as for analogue broadcasting. Many existing TV receivers are able to receive the EWS signal. In the case of analogue TV receivers, these turn on automatically when the TV receiver detects the EWS signal, even if the switch is set to off, and the viewer can obtain the urgent information. However, digital TV receivers can receive this signal only when the switch of the TV receivers is turned on, under the current situation.

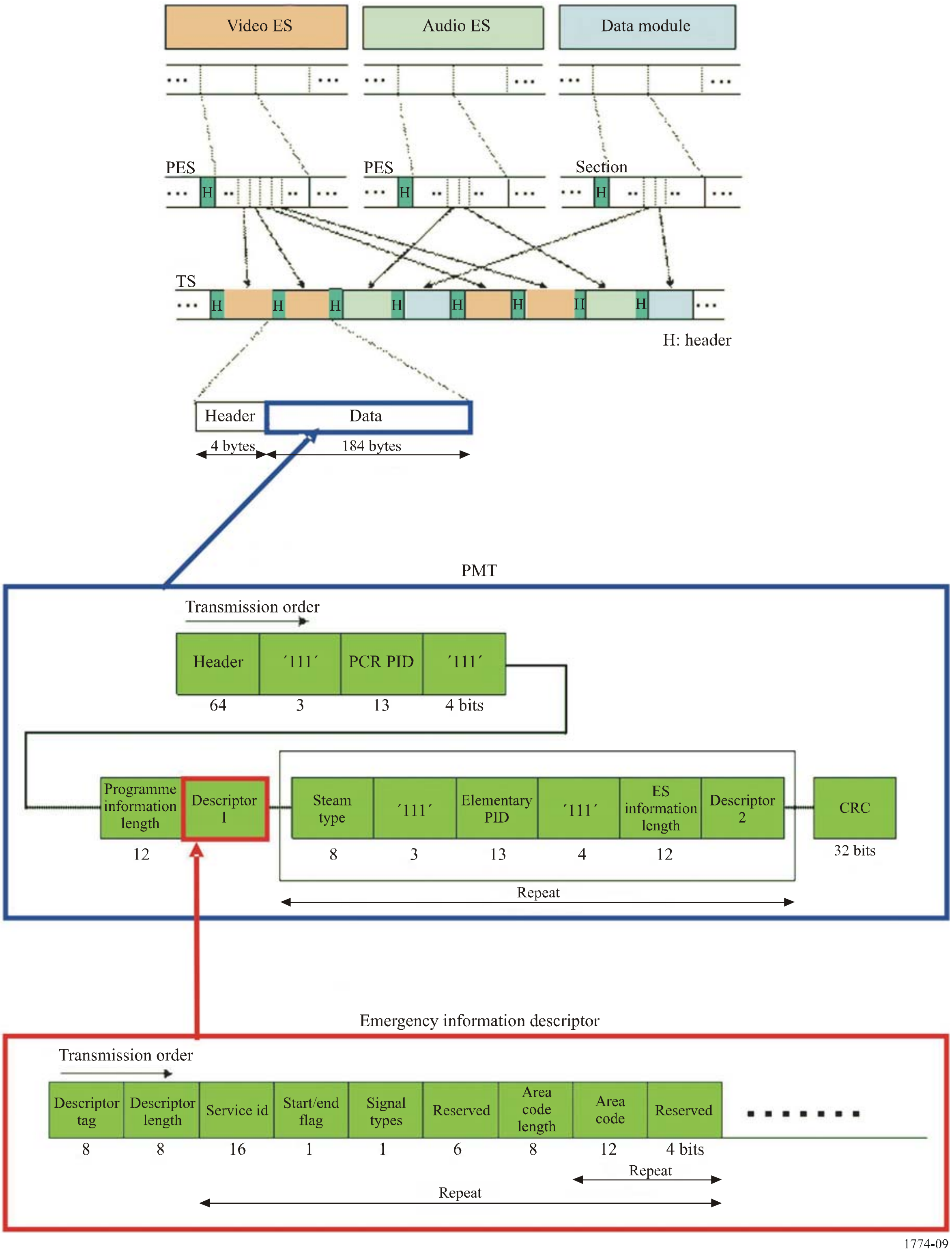
Fundamentally, the operation when the EWS signal is received is established by the product specification of each manufacturer.

2.4.1 Technical specifications of digital EWS

The emergency information descriptor may be used only for ISDB-TSB recommended in Recommendation ITU-R BS.1114 (System F), ISDB-T recommended in Recommendation ITU-R BT.1306 (System C), broadcasting-satellite service (sound) system using the 2.6 GHz band recommended in Recommendation ITU-R BO.1130 (System E), and ISDB-S recommended in Recommendation ITU-R BO.1408. The emergency information descriptor for EWS is placed in the Descriptor 1 field of the programme map table (PMT), which is periodically placed in the transport stream (TS). The details of the emergency information descriptor is shown in Fig. 9.

FIGURE 9

Structures of TS, PMT and emergency information descriptor



Notes to Fig. 9:

1 *ES (elementary stream):* ES is encoded video and audio, etc.

2 *PES (packetized elementary stream):* PES is packetized ES in each significant unit.

3 *TS (transport stream):* TS is divided PES, and the size is 188 bytes including 32 bytes of the header.

4 *PID (packet identifier):* PID shows what the transmitted packet is.

5 *CRC (cyclic redundancy check):* CRC is a type of hash function used to produce a checksum, which is a small number of bits, from a large block of data, such as a packet of network traffic or a block of a computer file, in order to detect errors in transmission or storage.

6 *Descriptor tag:* The value of the descriptor tag shall be $0 \times FC$, representing the emergency information descriptor.

7 *Descriptor length:* The descriptor length shall be a field that writes the number of data bytes following this field.

8 *Service id:* The service id shall be used to identify the broadcast programme number.

9 *Start/end flag:* The value of the start/end flag shall be '1' and '0', respectively, when transmission of emergency information signal starts (or is currently in progress) or when transmission ends.

10 *Signal types:* The value of the signal type must be '0' and '1', respectively, for Category I and II start signals.

11 *Area code length:* The area code length shall be a field that writes the number of data bytes following this field.

12 *Area code:* The area code shall be a field transmitting the area code.

2.4.2 Mobile and portable reception

In Japan, digital terrestrial television broadcasting for mobile and portable reception using one of 13 segments will be launched in early 2006. Digital EWS for mobile and portable reception is the same as described in § 5.1, but the actual receiver is under development.

In digital reception with a mobile terminal, such as cellular phone or PDA (portable digital assistant), the following effects are expected in the disaster prevention field:

- realize a congestion-free transmission path even in times of disaster;
- realize stable information transmission even in times of emergency or disaster, through start-up control;
- realize communication paths according to areas and targets.

2.4.3 Automatic activation of handheld receivers by EWS signals

Digital terrestrial broadcasting has an emergency warning mechanism similar to that of analogue broadcasting. Broadcasting differs from telecommunications in that it can send information to a large number of handheld receivers at the same time. The ability to activate handheld receivers to receive emergency information would lead to a reduction in the damage caused by a disaster. For this to be effective, a handheld receiver would have to be in the constant stand-by mode for the EWS signals, but if the power consumption were too high, it would be difficult to maintain stand-by for a long time.

To solve this problem, a low-power-consumption EWS signal stand-by circuit that can maintain stand-by for the digital terrestrial broadcasting EWS signals have been studied.

FIGURE 10

A concept of digital EWS for mobile and portable reception

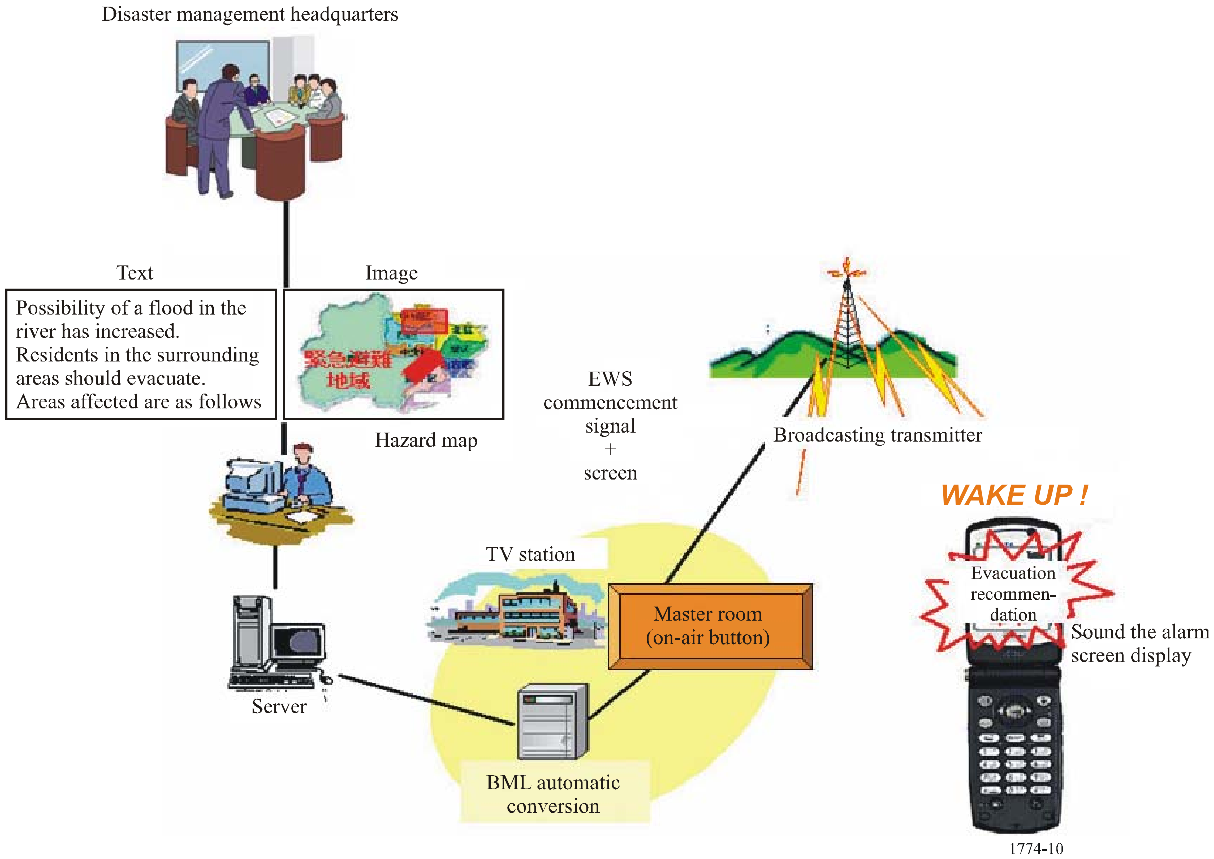


Figure 11 shows handheld receiver activation using EWS signals for digital terrestrial broadcasting.

An EWS signal is indicated by bit 26 of the transmission and multiplexing configuration control (TMCC) signals comprising 204 bits in System C of Recommendation ITU-R BT.1306. In the case of Mode 3 (number of carriers: 5 617), the number of TMCC carriers is 52 in total for 13 segments, or four carriers per segment. The TMCC signals modulated by differential binary phase shift keying (DBPSK) are transmitted at an interval of approximately 0.2 s.

To achieve remote activation, the EWS signals in one or more TMCC carriers are to be continuously monitored by each receiver. Furthermore, continuous monitoring shall be achieved without substantially shortening the stand-by time of handheld receivers. To reduce the power consumption, a dedicated stand-by algorithm is introduced that:

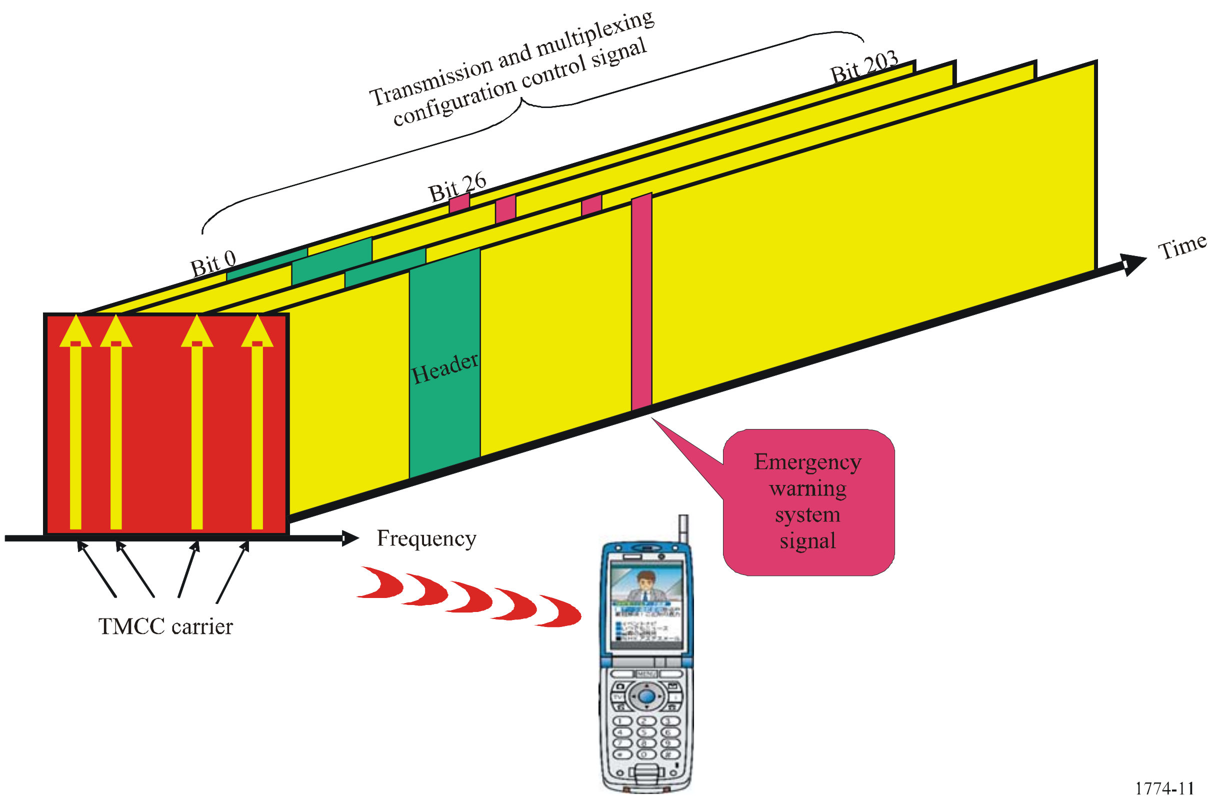
– extracts only TMCC carriers, and
– monitors only the EWS signals by limiting time slots.

The function for EWS stand-by with very low power consumption has been verified.

The remote activation technique which uses the EWS signals in TMCC can also be applied to fixed receivers of System C of Recommendation ITU-R BT.1306.

FIGURE 11

Handheld receiver activation using EWS signals of digital terrestrial broadcasting



2.5 Bibliography (informative)

The information on the Emergency Warning System is available in the following references.

ARIB Standard, BTA R-001 Receiver for Emergency Warning System (EWS): (http://www.arib.or.jp/english/).

ARIB Standard, ARIB STD-B32 Video Coding, Audio Coding and Multiplexing Specifications for Digital Broadcasting: (http://www.arib.or.jp/english/)

ARIB Technical Report, ARIB TR-B14 Operational Guidelines for Digital Terrestrial Television Broadcasting: (http://www.arib.or.jp/english/).

REPORT ITU-R M.2033

Radiocommunication objectives and requirements for public protection and disaster relief

(2003)

1 Scope

The purpose of the Report is to define the public protection and disaster relief (PPDR) objectives and requirements for the implementation of future advanced solutions to satisfy the operational needs of PPDR organizations around the year 2010. Specifically, it identifies objectives, applications, requirements, a methodology for spectrum calculations, spectrum requirements and solutions for interoperability.

This Report has been developed in preparation for WRC-03 agenda item 1.3:

> "to consider identification of globally/regionally harmonized bands, to the extent practicable, for the implementation of future advanced solutions to meet the needs of public protection agencies, including those dealing with emergency situations and disaster relief, and to make regulatory provisions, as necessary, taking into account Resolution **645 (WRC-2000)**."

Resolution 645 (WRC-2000) invited the ITU-R to "study, as a matter of urgency, identification of frequency bands that could be used on a global/regional basis by administrations intending to implement future solutions for public protection agencies and organizations, including those dealing with emergency situations and disaster relief;" and "to study, as a matter of urgency, regulatory provisions necessary for identifying globally/regionally harmonized frequency bands for such purposes;". Resolution 645 (WRC-2000) also invited the ITU-R to "... conduct studies for the development of a resolution identifying the technical and operational basis for global cross-border circulation of radiocommunication equipment in emergency and disaster relief situations,". Recommendation ITU-R M.1637 provides additional guidance on this element.

2 Background

Radiocommunications have become extremely important to public protection and disaster relief (PPDR) organizations to the extent that PPDR communications are highly dependent upon it. At times, radiocommunication is the only form of communications available.

In order to provide effective communications, PPDR agencies and organizations have a set of objectives and requirements that include interoperability, reliability, functionality, security in operation and fast call set-up[1] in each area of operation. Considering that the radiocommunication needs of PPDR agencies and organizations are growing, future advanced solutions used by PPDR will require higher data rates, along with video and multimedia capability.

[1] Fast call set-up indicates reducing the response time to access the particular network.

This Report forms part of the process of specifying these objectives and the requirements of PPDR organizations to meet their future needs. PPDR organizations will operate their communications in a complex environment, which requires the recognition of the following factors:

a) the involvement of a number of interests (such as governments, service providers, manufacturers);

b) the changing regulatory framework for those involved in supplying systems supporting PPDR;

c) that PPDR applications may be narrowband, wideband or broadband, or a mixture of these;

d) the need for interoperability and interworking between networks;

e) the need for high levels of security;

f) the needs of developing countries;

g) the ITU-D Handbook on Disaster Communications;

h) the needs of countries, particularly for developing countries, for low-cost communications equipment for public protection and disaster relief agencies and organizations;

i) that the 1998 Intergovernmental Conference on Emergency Telecommunications (ICET-98), with the participation of 76 countries and various intergovernmental and non-governmental organizations, adopted the Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations. In 1998, thirty-three States signed this comprehensive Convention that also contains an article dealing with the removal of regulatory barriers;

j) that the *Working Group on Emergency Telecommunications* (WGET), which is also the *Reference Group on Telecommunications (RGT)* of the *Inter-Agency Standing Committee (IASC)* on humanitarian affairs has adopted frequencies in the VHF and UHF bands allocated to the land mobile service for inter-agency coordination of relief operations and safety and security communications in international humanitarian assistance as listed in Annex 3 to this Report;

k) that many disaster relief organizations require independence to fulfill their humanitarian mandate by maintaining their operational autonomy while fully respecting the laws of the countries in which they operate;

l) that in times of disasters, when most terrestrial based networks may be destroyed or impaired, amateurs, satellite and other non-ground based networks may be able to provide communications services to assist in public protection and disaster relief efforts;

m) that systems operating within various radiocommunication services, including mobile, fixed, mobile satellite, fixed satellite and/or amateur, could support both current and future advanced PPDR applications;

n) that in some countries, national regulations and/or legislation may affect the ability of PPDR organizations to use commercial wireless systems or networks;

o) that in some countries, commercial wireless systems currently offer and will probably continue to support PPDR applications;

p) that there is potential for new technologies such as IMT-2000 systems and beyond, and intelligent transportation systems (ITS), which may support or supplement advanced PPDR applications and that such complementary use would be in response to market demands.

3 Harmonization of spectrum

Significant amounts of spectrum are already in use in various bands in various countries for narrowband PPDR applications, however, it should be noted that sufficient spectrum capacity will be required to accommodate future operational needs including narrowband, wideband and broadband applications. Experience has shown that spectrum that is harmonized has benefits that include economic benefits, the development of compatible networks and effective services and the promotion of interoperability of equipment internationally and nationally for those agencies that require national and cross-border cooperation with other PPDR agencies and organizations. Specifically, some potential benefits are as follows:

– economies of scale in the manufacturing of equipment;

– competitive market for equipment procurement;

– increased spectrum efficiency;

– stability in band planning, that is, evolving to globally/regionally harmonized spectrum arrangements may assist in more efficient planning of land mobile spectrum; and

– increased effective response to disaster relief.

When considering appropriate frequencies for PPDR, it should be recognized that the propagation characteristics of lower frequencies allow them to travel farther than higher frequencies, making low frequency systems potentially less costly to deploy in rural areas. Lower frequencies are also sometimes preferred in urban settings due to their superior building penetration. However, these lower frequencies have become saturated over time and to prevent overcrowding some administrations now use more than one frequency band in different parts of the radio spectrum.

The more bands that may be identified with different propagation characteristics the more difficult it becomes to benefit from economies of scale. Therefore, a balance needs to be struck between the number and location of the bands identified.

4 Aspects of frequency bands for PPDR

Based upon an ITU-R survey of PPDR communications conducted in the 2000-2003 study period from over 40 ITU members and international organizations and consequent considerations, the following comments should be noted:

a) There is little uniformity in regard to frequency bands that are used for PPDR in different countries.

b) While in most countries the bands used for public protection are the same as those used for disaster relief, in some countries separate bands are used.

c) Many administrations have designated one or more frequency bands for narrowband PPDR operations. It should be noted that only particular sub-bands of the frequency ranges or parts thereof listed below are utilized in an exclusive manner for PPDR radiocommunications: 3-30 MHz, 68-88 MHz, 138-144 MHz, 148-174 MHz, 380-400 MHz (including CEPT designation of 380-385/390-395 MHz), 400-430 MHz, 440-470 MHz, 764-776 MHz, 794-806 MHz, and 806-869 MHz (including CITEL designation of 821-824/866-869 MHz). One administration has designated PPDR spectrum for wideband and broadband applications.

d) Some administrations in Region 3 are using or plan to use or have identified parts of the frequency bands 68-88 MHz, 138-144 MHz, 148-174 MHz, 380-399.9 MHz, 406.1-430 MHz and 440-502 MHz, 746-806 MHz, 806-824 MHz and 851-869 MHz for PPDR applications. Some administrations in Region 3 are also using the bands 380-399.9 MHz, 746-806 MHz and 806-824 MHz paired with 851-869 MHz for Government communications.

The bands which are listed in § c) and d) above and other potential candidate bands are discussed in detail in the CPM-02 Report (§ 2.1.2.6) together with their advantages and disadvantages and are listed in Annex 2.1-1 of the CPM-02 Report.

5 Summary

Based on the studies undertaken in ITU-R on PPDR, this Report focuses on the numerous radio-communication objectives and requirements that may be required to support future advanced solutions for PPDR applications. The following areas of interest were generated during the process of developing this report:

Annex 1 Radiocommunication objectives for public protection and disaster relief

Annex 2 Radiocommunication requirements for public protection and disaster relief

Annex 3 Narrowband frequencies for inter-agency coordination and safety and security communications in international humanitarian assistance presently in use

Annex 4 Spectrum requirements for public protection and disaster relief

Annex 5 Existing and emerging solutions to support interoperability for public protection and disaster relief

Annex 1

Radiocommunication objectives for public protection and disaster relief

1 General objectives

Public protection and disaster relief (PPDR) radiocommunication systems aim to achieve the following general objectives:

a) to provide radiocommunications that are vital to the achievement of:
   - the maintenance of law and order;
   - response to emergency situations and protection of life and property;
   - response to disaster relief situations;

b) to provide the services as identified above in item a) over a wide range of geographic coverage areas, including urban, suburban, rural and remote environments;

c) to aid the provision of future advanced solutions requiring high data rates, video and multimedia used by PPDR agencies and organizations;

d) to support interoperability and interworking between networks, both nationally and for cross-border operation, in emergency and disaster relief situations;

e) to allow international operation and roaming of mobile and portable units;

f) to make efficient and economical use of the radio spectrum, consistent with providing services at an acceptable cost;

g) to accommodate a variety of mobile terminals from those which are small enough to be carried on one's person to those which are mounted on vehicles;

h) to encourage the cooperation between countries for the provision of effective and appropriate humanitarian assistance during disaster relief situations;

i) to make available PPDR radiocommunications at reasonable costs in all markets;

j) to support the needs of developing countries, including the provision for low-cost solutions for PPDR agencies and organizations.

2 Technical objectives

Systems for PPDR aim to achieve the following technical objectives:

a) to support the integration of voice, data, and image communication;

b) to provide additional level(s) of security associated with the type of information carried over the communication channels associated with the various PPDR applications and operations;

c) to support equipment that operates in extreme and diverse operational conditions (rough road, dust, extreme temperature, etc.);

d) to accommodate the use of repeaters for covering long distances between terminals and base stations in rural and remote areas and also for intensive on-scene localized areas;

e) to provide fast call set-up, one touch broadcasting and group call features.

3 Operational objectives

Systems for PPDR aim to achieve operational objectives, including the following:

a) to provide security including end-to-end encryption, terminal/network authentication;

b) to enable communications management to be controlled by PPDR agencies and organizations such as instant/dynamic reconfiguration change, set-up talk groups, guaranteed access including priority and pre-emption calls, groups or general calls, spectrum resource availability for multiple PPDR agencies and organizations, coordination and rerouting;

c) to provide communications through the system/network and/or independent of the network such as direct mode operation (DMO), simplex radio and push-to-talk;

d) to provide customized and reliable coverage especially for indoor areas such as underground and inaccessible areas. To also allow for the extension of cell size or capacity in rural and remote areas or under severe conditions during emergency and disaster situations;

e) to provide full service continuity through measures such as redundancy for emergency operations, prompt capacity increase to survive partial loss of infrastructure crucial to effective mission compliance and the safety and security of PPDR personnel;

f) to provide high quality of service including instant call set-up and instant push-to-talk, resilience under extreme load, very high call set-up success rate, etc.

g) to take account of various PPDR applications.

Annex 2

Radiocommunication requirements for public protection and disaster relief

1 Terminology

1.1 Public protection and disaster relief (PPDR)

There are terminology differences between administrations and regions in the scope and specific meaning of PPDR. The following terms are appropriate for the purpose of discussing this issue:

– *Public protection (PP) radiocommunication*: Radiocommunications used by responsible agencies and organizations dealing with maintenance of law and order, protection of life and property, and emergency situations.

– *Disaster relief (DR) radiocommunication*: Radiocommunications used by agencies and organizations dealing with a serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as a result of complex, long-term processes.

1.2 Applicability of voice, data, graphics and video to global/regional PPDR

As PPDR operations become more reliant on electronic databases and data processing, access to accurate and detailed information by staff in the field such as police, firefighters and medical emergency personnel is critical to improving the effectiveness of the staff in resolving emergency situations. This information is typically held in office based database systems and includes images, maps, architectural plans of buildings, and locations of hazardous materials systems.

In the other direction, the flow of information back from units in the field to operational control centres and specialist knowledge centres is equally important. Examples to note are the remote monitoring of patients and remote real-time video monitoring of civil emergency situations including the use of remote control robotic devices. Moreover, in disaster and emergency situations, critical decisions to be made by controlling authorities are often impacted by the quality and timeliness of the information received from the field.

These applications in general require higher bit-rate data communications than can be provided by current PPDR applications. The availability of future advanced solutions is expected to be of benefit to PPDR operations.

1.3 Consideration of advantages with future technologies

While voice communications will remain a critical component of PPDR operations, new data and video services will play a key role. For instance, PPDR agencies today use applications such as video for surveillance of crime scenes and of highways, to monitor and conduct damage assessment of wild land fire scenes from airborne platforms to provide real-time video back to emergency command centres. Also, there is a growing need for full motion video for other uses such as robotic devices in emergency situations. These types of future advanced solutions will be capable of providing local voice, video and data networks, thereby serving the needs of emergency personnel responding to an incident.

If these future technologies were implemented globally, it could reduce the cost of equipment, increase availability of equipment, increase potential for interoperability, may provide for a wider range of capabilities and reduce network infrastructure rollout time.

Introduction of these technologies may enable PPDR agencies and organizations to keep up with increasing demands but also may enable them to implement advanced voice, text, video and other intensive data applications and services designed to enhance service delivery. In this regard, it should be noted that any development or planning for the use of future technologies may require that consideration be given to spectrum aspects for PPDR applications.

If PPDR applications used IMT-2000 technology, it may be possible to use commercial IMT-2000 networks in regions where it was not cost-effective to deploy a dedicated network. IMT-2000 is intended for deployment in a wide range of environments, from rural to the densest urban areas. Commercial systems that are being deployed using IMT-2000 technologies may not meet all of the identified needs for PPDR. However, the use of these technologies and systems should be considered, particularly in terms of the potential associated cost savings and advanced features that they offer.

1.4 Narrowband, wideband, broadband

Communications supporting PPDR operations cover a range of radiocommunication services such as fixed, mobile, amateur and satellite. Typically, narrowband technologies are used for PPDR communications within the terrestrial mobile service, while wideband and broadband technologies are finding PPDR applications within all radiocommunication services.

There are some differences between administrations and regions in the scope and specific meaning of narrowband, wideband and broadband. However, the ITU-R considers the terms described in § 1.4.1, 1.4.2 and 1.4.3 appropriate for the purpose of discussing this issue:

1.4.1 Narrowband (NB)

To provide PPDR narrowband applications, the trend is to implement wide area networks including digital trunked radio networks providing digital voice and low speed data applications (e.g. pre-defined status messages, data transmissions of forms and messages, access to databases). ITU Report ITU-R M.2014 lists a number of technologies, with typical channel bandwidths up to 25 kHz, that are currently used to deliver narrowband PPDR applications. Some countries do not mandate specific technology, but promote the use of spectrum-efficient technology.

1.4.2 Wideband (WB)

It is expected that the wideband technologies will carry data rates of several hundred kilobits per second (e.g. in the range of 384-500 kbit/s). Since it is expected that networks and future technologies may require higher data rates, a whole new class of applications including: wireless transmission of large blocks of data, video and Internet protocol-based connections in mobile PPDR may be introduced.

The use of relatively high-speed data in commercial activities gives a wide base of technology availability and will therefore spur the development of specialist mobile data applications. Short message and e-mail are now being seen as a fundamental part of any communications control and command system and therefore could most likely be an integral part of any future PPDR capability.

A wideband wireless system may be able to reduce response times of accessing the Internet and other information databases directly from the scene of an incident or emergency. It is expected that this will initiate the development of a range of new and secure applications for PPDR organizations.

Systems for wideband applications to support PPDR are under development in various standards organizations. Many of these developments are referenced in Report ITU-R M.2014 and in Recommendations ITU-R M.1073, ITU-R M.1221 and ITU-R M.1457 and with channel bandwidths dependent on the use of spectrally efficient technologies.

1.4.3 Broadband (BB)

Broadband technology could be seen as a natural evolutionary trend from wideband. Broadband applications enable an entirely new level of functionality with additional capacity to support higher speed data and higher resolution images. It should be noted that the demand for multimedia capabilities (several simultaneous wideband and/or broadband applications running in parallel) puts a huge demand with very high bit rates on a wireless system deployed in a localized area with intensive on-scene requirements (often referred to as "hot spot" areas) where PPDR personnel are operating.

Broadband applications could typically be tailored to service localized areas (e.g. 1 km^2 or less) providing voice, high-speed data, high quality digital real time video and multimedia (indicative data rates in range of 1-100 Mbit/s) with channel bandwidths dependent on the use of spectrally efficient technologies. Examples of possible applications include:

– high-resolution video communications from wireless clip-on cameras to a vehicle-mounted laptop computer, used during traffic stops or responses to other incidents and video surveillance of security entry points such as airports with automatic detection based on reference images, hazardous material or other relevant parameters;

– remote monitoring of patients and remote real-time video view of the single patient demanding up to 1 Mbit/s. The demand for capacity can easily be envisioned during the rescue operation following a major disaster. This may equate to a net hot spot capacity of over 100 Mbit/s.

Broadband systems may have inherent noise and interference tradeoffs with data rates and associated coverage. Depending on the technology deployed, a single broadband network may have different coverage areas in the range of a few metres up to hundreds of metres, providing a wide range in spectrum reuse capability. Collectively, the high data speeds and localized coverage area open up numerous new possibilities for PPDR applications (tailored area networks, hot spot deployment and ad-hoc networks).

Finally, it should be noted that various standards organizations are beginning work on systems for broadband applications including Project MESA.

2 Radio operating environments for PPDR

Various radio operating environments are applicable to PPDR and are explained in this section. The purpose of further explaining distinct radio operating environments is to define scenarios that, from the radio perspective, may impose different requirements on the use of PPDR applications and their importance.

The identified PPDR scenarios could serve as the basis for identifying PPDR requirements and may complement the estimates for spectrum.

The scenarios include average day-to-day operations, large emergencies or public events and disasters. These have been identified since they are distinct in terms of the characteristics and may impose different requirements for PPDR communications.

2.1 Day-to-day operations

Day-to-day operations encompass the routine operations that PPDR agencies conduct within their jurisdiction. Typically, these operations are within national borders. Generally, most PP spectrum and infrastructure requirements are determined using this scenario with extra capacity to cover unspecified emergency events. For the most part day-to-day operations are minimal for DR. In Tables 2 and 3, day-to-day operations are referred to as PP (1).

2.2 Large emergency and/or public events

Large emergencies and/or public events are those that PP and potentially DR agencies respond to in a particular area of their jurisdiction; however they are still required to perform their routine operations elsewhere within their jurisdiction. The size and nature of the event may require additional PPDR resources from adjacent jurisdictions, cross-border agencies, or international organizations. In most cases, there are either plans in place or there is some time to plan and coordinate the requirements.

A large fire encompassing 3-4 blocks in a large city (e.g. New York, New Delhi) or a large forest fire are examples of a large emergency under this scenario. Likewise, a large public event (national or international) could include the Commonwealth Heads of Government Meeting (CHOGM), G8 Summit, the Olympics, etc.

Generally, additional radiocommunications equipment for large events is brought to the area as required. This equipment may or may not be linked into the existing PP network infrastructure.

In Tables 2 and 3, large emergencies or public events are referred to as PP (2).

2.3 Disasters

Disasters can be those caused by either natural or human activity. For example, natural disasters include an earthquake, major tropical storm, a major ice storm, floods, etc. Examples of disasters caused by human activity include large-scale criminal incidences or situations of armed conflict. Generally, both the existing PP communications systems and special on-scene communications equipment brought by DR organizations are employed.

Even in areas where suitable terrestrial services exist, MSS systems will play a significant role in disaster situation. The terrestrial services which do exist may have been damaged by the disaster itself, or may be unable to cope with the increased traffic demands resulting from a disaster situation. In these situations, satellite solutions can offer a reliable solution. The frequency bands used by MSS systems are generally harmonised at a global level. However, the cross border circulation of terminals in disaster situations is a critical issue, as recognised in the Tampere Convention. It is imperative that neighbouring countries that may hold MSS terminals as part of their contingency planning are able to offer the initial essential communications required with minimum delay. To this end, advanced bilateral and multilateral agreements are desirable and may be accomplished through, for example the GMPCS-MoU.

Some PPDR agencies/organizations and amateur radio groups use HF narrowband systems including the use of data modes of operation as well as voice. Other technologies such as digital voice, high-speed data and video are in early implementations either using terrestrial or satellite network services.

In Tables 2 and 3, disasters are referred to as DR.

3 Requirements

Tables 2 and 3 summarize § 3.1 and 3.2, which describe PPDR application and user requirements.

When considering these sections, it is important to note that public protection organizations currently use various arrangements of mobile systems or a combination thereof, as described below in Table 1.[2]

TABLE 1

Arrangements of mobile systems used by public protection

Item	Network ownership	Operator	User(s)	Spectrum assignment
a	PP organization	PP organization	PP exclusive	PP
b	PP organization	Commercial	PP exclusive	PP
c	Commercial	Commercial	PP exclusive	PP or commercial
d	Commercial	Commercial	Shared with PP priority	PP or commercial
e	Commercial	Commercial	Shared with PP treated as ordinary customer	Commercial

Items b), c), d) and e) of Table 1 in some countries are currently used by PP organizations to supplement their own systems or in some cases to provide all their communications requirements, but not necessarily all the items specified in Tables 2 and 3. It is likely that this trend will continue into the future, particularly with the introduction of advanced wireless solutions, such as IMT-2000.

Some of the applications listed in § 3.1.3 and Table 2 may depend significantly on commercial systems, while other applications for the same PP organizations may be totally independent of commercial systems.

3.1 Applications

3.1.1 General

a) Applications associated with the routine day-to-day and emergency operations for public protection applications as outlined in Table 2 could be offered.

b) Applications associated with disaster relief operations as outlined in Table 2 could be offered.

c) Regional and/or international harmonization of spectrum for the provision of PPDR applications could be allowed if a requirement is determined for this need.

d) Applications for PPDR could be developed to support a variety of user terminals including handheld and vehicle-mounted.

e) The description of environments for PPDR is provided in § 2 of this Annex.

3.1.2 Application accessibility requirements

The eventual accessibility of applications for PPDR may depend on various issues. These include the cost, the regulatory and the national legislative climate, the nature of mandates PPDR, and the need of the area to be served. The exact applications and particular features to be provided by the various PPDR organizations are to be decided by such organizations.

2 Examples of the types of mobile systems can be found in Recommendations ITU-R M.1073, ITU-R M.1457 and in Report ITU-R M.2014.

TABLE 2

Arrangements of mobile systems used by public protection

Application	Feature	PPDR Example	Importance(1)		
			PP (1)	PP (2)	DR
1. *Narrowband*					
Voice	Person-to-person	Selective calling and addressing	H	H	H
	One-to-many	Dispatch and group communication	H	H	H
	Talk-around/direct mode operation	Groups of portable to portable (mobile-mobile) in close proximity without infrastructure	H	H	H
	Push-to-talk	Push-to-talk	H	H	H
	Instantaneous access to voice path	Push-to-talk and selective priority access	H	H	H
	Security	Voice encryption/scrambling	H	H	M
Facsimile	Person-to-person	Status, short message	L	L	H
	One-to-many (broadcasting)	Initial dispatch alert (e.g. address, incident status)	L	L	H
Messages	Person-to-person	Status, short message, short e-mail	H	H	H
	One-to-many (broadcasting)	Initial dispatch alert (e.g. address, incident status)	H	H	H
Security	Priority/instantaneous access	Man down alarm button	H	H	H
Telemetry	Location status	GPS latitude and longitude information	H	M	H
	Sensory data	Vehicle telemetry/status	H	H	M
		EKG (electrocardiograph) in field	H	H	M
Database interaction (minimal record size)	Forms based records query	Accessing vehicle license records	H	H	M
		Accessing criminal records/missing person	H	H	M
	Forms based incident report	Filing field report	H	H	H
2. *Wideband*					
Messages	E-mail possibly with attachments	Routine e-mail message	M	M	L
Data Talk-around/direct mode operation	Direct unit to unit communication without additional infrastructure	Direct handset to handset, on-scene localized communications	H	H	H
Database interaction (medium record size)	Forms and records query	Accessing medical records	H	H	M
		Lists of identified person/missing person	H	H	H
		GIS (geographical information systems)	H	H	H
Text file transfer	Data transfer	Filing report from scene of incident	M	M	M
		Records management system information on offenders	H	M	L
		Downloading legislative information	M	M	L
Image transfer	Download/upload of compressed still images	Biometrics (finger prints)	H	H	M
		ID picture	H	H	M
		Building layout maps	H	H	H
Telemetry	Location status and sensory data	Vehicle status	H	H	H
Security	Priority access	Critical care	H	H	H

TABLE 2 (*end*)

Application	Feature	PPDR Example	Importance(1)		
			PP (1)	PP (2)	DR
Video	Download/upload compressed video	Video clips	M	L	L
		Patient monitoring (may require dedicated link)	M	M	M
		Video feed of in-progress incident	H	H	M
Interactive	Location determination	2-way system	H	H	M
		Interactive location data	H	H	H
3. *Broadband*					
Database access	Intranet/Internet access	Accessing architectural plans of buildings, location of hazardous materials	H	H	H
	Web browsing	Browsing directory of PPDR organization for phone number	M	M	L
Robotics control	Remote control of robotic devices	Bomb retrieval robots, imaging/video robots	H	H	M
Video	Video streaming, live video feed	Video communications from wireless clip-on cameras used by in building fire rescue	H	H	H
		Image or video to assist remote medical support	H	H	H
		Surveillance of incident scene by fixed or remote controlled robotic devices	H	H	M
		Assessment of fire/flood scenes from airborne platforms	M	H	M
		Assessment of fire/flood scenes from airborne platforms	M	H	M
Imagery	High resolution imagery	Downloading Earth exploration-satellite images	L	L	M
		Real-time medical imaging	M	M	M

(1) The importance of that particular application and feature to PPDR is indicated as high (H), medium (M), or low (L). This importance factor is listed for the three radio operating environments: "Day-to-day operations", "Large emergency and/or public events", and "Disasters", represented by PP (1), PP (2) and DR, respectively.

3.1.3 Envisioned applications

Table 2 lists the envisioned applications with particular features and specific PPDR examples. The applications are grouped under the narrowband, wideband or broadband headings to indicate which technologies are most likely to be required to supply the particular application and their features. Furthermore, for each example, the importance (high, medium or low) of that particular application and feature to PPDR is indicated. This importance factor is listed for the three radio operating environments identified in Annex 2, § 2.1 "Day-to-day operations", § 2.2 "Large emergency and/or public events", and § 2.3 "Disasters", represented by PP (1), PP (2) and DR, respectively.

3.2 User requirements

This section includes the requirements from the perspective of the PPDR end users. General technology, functional and operational requirements are described. Although some of the requirements do not relate specifically to the radiocommunication network or system used by PPDR, they do affect the design, implementation and use of radiocommunications.

Table 3, at the end of this section, is a general summary of the user requirements. The requirements are grouped under the same headings as § 3.2.1 through 3.2.8 and any key attributes related to the requirement are listed in the second column. Furthermore, the importance (high, medium or low) of that particular requirement to PPDR is indicated. This importance factor is listed for the three radio operating environments identified in § 2.1 "Day-to-day operations", § 2.2 "Large emergency and/or public events", and § 2.3 "Disasters", represented by PP (1), PP (2) and DR, respectively.

The detailed choice of PPDR applications and features to be provided in any given area by PPDR is a national or operator specific matter. However, the capabilities of the service are affected by the following requirements.

3.2.1 System requirements

3.2.1.1 Support of multiple applications

As desired by PPDR organizations, systems serving PPDR should be able to support a broad range of applications, as identified in § 3.2.

3.2.1.2 Simultaneous use of multiple applications

As desired by the PPDR organization, systems serving PPDR should be able to support the simultaneous use of several different applications with a range of bit rates.

Some PPDR users may require the integration of multiples applications (e.g. voice and low/medium speed data) over the complete network or on a high speed network to service localized areas with intensive on-scene activity.

3.2.1.3 Priority access

As desired by the PPDR organizations, systems serving PPDR should have the ability to manage high priority traffic and possibly manage low priority traffic load shedding during high traffic situations. PPDR may require the exclusive use of frequencies or equivalent high priority access to other systems.

3.2.1.4 Grade of service (GoS) requirements

Suitable grade of service should be provided for PPDR applications.

PPDR users may also require reduced response times for accessing the network and information directly at the scene of incidence, including fast subscriber/network authentication.

3.2.1.5 Coverage

The PPDR system is usually required to provide complete coverage (for "normal" traffic within the relevant jurisdiction and/or operation (national, provincial/state or at the local level). This coverage is required 24 h/day, 365 days/year.

Usually, systems supporting PPDR organizations are designed for peak loads and wide fluctuations in use. Additional resources, enhancing system capacity may be added during a PP emergency or DR event by techniques such as reconfiguration of networks with intensive use of DMO and vehicular repeaters (NB, WB, BB), which may be required for coverage of localized areas.

Systems supporting PPDR are also usually required to provide reliable indoor and outdoor coverage, coverage of remote areas, and coverage of underground or inaccessible areas (e.g. tunnels, building basements). Appropriate redundancy to continue operations when the equipment/infrastructure fails is extremely beneficial.

PPDR systems are not generally installed inside numerous buildings. PPDR entities do not have a continuous revenue stream to support installation and maintenance of an intensive variable density infrastructure. Urban PPDR systems are designed for highly reliable coverage of personal stations outdoors with limited access indoors by direct propagation through the building walls. Sub-systems may be installed in specific building or structures, like tunnels, if penetration through the walls is insufficient. PPDR systems tend to use larger radius cells and higher power mobile and personal stations than commercial service providers.

3.2.1.6 Capabilities

PPDR users require control (full or in part) of their communications, including centralized dispatch (command and control center), access control, dispatch group (talk group) configuration, priority levels, and pre-emption (override other users).

Rapid dynamic reconfiguration of the system serving PPDR may be required. This includes robust operation administration and maintenance (OAM) offering status and dynamic reconfiguration. System capability of over-the-air programmability of field units is extremely beneficial.

Robust equipment (e.g. hardware, software, operational and maintenance aspects) are required for systems serving PPDR. Equipment that functions while the user is in motion are also required. Equipment may also require high audio output (high noise environment), unique accessories, such as special microphones, operation while wearing gloves, operation in hostile environments (heat, cold, dust, rain, water, shock, vibration, explosive environments, etc.) and long battery life.

PPDR users may require the system to have capability for fast call set-up, instant push-to-talk operations or one touch broadcasting/group call. Talk-around (direct mode, simplex), communications to aircraft and marine equipment, control of robotic devices, vehicular repeater (on-scene repeater, extend network to remote locations) may also be required.

As the trend continues to move towards IP based solutions, PPDR systems may be required to be IP compatible or be able to interface with IP based solutions.

Appropriate levels of interconnection to the public telecommunications network may also be required[3]. The decision regarding the level of interconnection (i.e. all mobile terminals vs. a percentage of terminals) may be based on the particular PPDR operational requirements. Furthermore, the specific access to the public telecommunications network (i.e. directly from mobile or through the PPDR dispatch) may also be based on the particular PPDR operational requirements.

There may be additional requirements for simulcast (quasi-synchronous broadcast), receiver operating (in-bound path diversity) that have not been covered in Table 3.

3.2.2 Security related requirements

Efficient and reliable PPDR communications within a PPDR organization and between various PPDR organizations, which are capable of secure operation, may be required.

Notwithstanding, there may be occasions where administrations or organisations, which need secure communications, bring equipment to meet their own security requirements.

Furthermore, it should be noted that many administrations have regulations limiting the use of secure communications for visiting PPDR users.

[3] A description of an international emergency preference scheme (IEPS) is described in ITU-T Recommendation E.106.

3.2.3 Cost related requirements

Cost effective solutions and applications are extremely important to PPDR users. These can be facilitated by open standards, a competitive marketplace, and economies of scale. Furthermore, cost effective solutions that are widely used can reduce the deployment costs of permanent network infrastructure.

3.2.4 Electromagnetic compatibility (EMC) requirements

Systems supporting PPDR should be in accordance with appropriate EMC regulations. Adherence to national EMC regulations may be required between networks, radiocommunications standards and co-located radio equipment.

3.2.5 Operational requirements

This section defines the operational and functional requirements for PPDR users and lists key attributes in Table 3.

3.2.5.1 Scenario

Greater safety of personnel can be accomplished through improved communications. Systems supporting PPDR should be able to operate in the various scenarios, as described in § 2. PPDR radiocommunication equipment should be able to support at least one of these operating environments, however, it is preferable that PPDR radiocommunication equipment support all of these radio operating environments. For any of these environments, information may be required to flow to and from units in the field to the operational control centre and specialist knowledge centres.

Although the type of operator for systems supporting PPDR is usually a regulatory and national matter, systems supporting PPDR may be satisfied by public or private operators.

PPDR systems and equipment capable of being deployed and set-up rapidly for large emergencies, public events and disasters (e.g. severe floods, large fires, the Olympics, peacekeeping) is extremely beneficial.

3.2.5.2 Interoperability

Interoperability is the seamless, coordinated, and integrated PPDR communications for the safe, effective, and efficient protection of life and property. Communications interoperability can be achieved at many levels of a PPDR operation. From the most basic level, i.e., a fire fighter of one organization communicating with a fire fighter of another, up to the highest levels of command and control.

Various options are available to facilitate communications interoperability between multiple agencies. These include, but are not limited to:

a) the use of common frequencies and equipment,

b) utilizing local, on-scene command vehicles/equipment/procedures,

c) via dispatch centres/patches, or

d) utilizing technologies such as audio switches or software defined radios. Typically multiple agencies use a combination of options.

Annex 5 provides a more detailed explanation of interoperability and possible solutions.

How these options are used to obtain interoperability depends how the PPDR organizations want to talk to each other and at what level in the organization. Usually, coordination of tactical communications between the on-scene or incident commanders of multiple public protection and disaster relief agencies is required.

Notwithstanding, while the importance of interoperability is recognised, PPDR equipment should be manufactured at a reasonable cost, while incorporating various aspects specific to each country/organization. Administrations should consider the cost implications of interoperable equipment since this requirement should not be so expensive as to preclude implementation within an operational context.

3.2.6 Spectrum usage and management

Depending on national frequency allocations, PPDR users must share with other terrestrial mobile users. The detailed arrangements regarding sharing of the spectrum vary from country to country. Furthermore, there may be several different types of systems supporting PPDR operating in the same geographical area. Therefore, interference to systems supporting PPDR from non-PPDR users should be minimized as much as possible.

Depending on the national regulations, systems supporting PPDR may be required to use specific channel spacing between mobile and base station transmit frequencies.

Each administration has the discretion to determine suitable spectrum for PPDR. Annexes 3 and 4 provide additional information on spectrum usage and requirements.

3.2.7 Regulatory compliance

Systems supporting PPDR should comply with the relevant national regulations. In border areas (near the boundary between countries), suitable coordination of frequencies should be arranged, as appropriate.

The capability of systems supporting PPDR to support extended coverage into the neighbouring country(ies) should also comply with regulatory agreements between the neighbours.

For disaster relief communications, administrations are encouraged to adhere to the principles of the Tampere Convention.

Flexibility should be afforded to PPDR users to employ various types of systems (e.g. HF, satellite, terrestrial, amateur, Global Maritime Distress and Safety System (GMDSS) at the scene of the incident in times of large emergencies and disasters.

3.2.8 Planning

Planning and pre-coordination activities can greatly support PPDR communications. Planning should take into account readily available equipment that could be provided for unpredictable events and disasters through existing inventory thereby reducing the reliance on supplies. It would be beneficial to maintain accurate and detailed information so that PPDR users can access this information at the scene.

Administrations have, or may also find it beneficial to have, provisions supporting national, state/provincial and local (e.g. municipal) systems.

TABLE 3

User requirements

Requirement	Specifics	Importance[(1)]		
		PP (1)	**PP (2)**	**DR**
1. *System*				
Support of multiple applications		H	H	M
Simultaneous use of multiple applications	Integration of multiple applications (e.g. voice and low/medium speed data)	H	H	M
	Integration of local voice, high speed data and video on high speed network to service localized areas with intensive on-scene activity	H	H	M
Priority access	Manage high priority and low priority traffic load shedding during high traffic	H	H	H
	Accommodate increased traffic loading during major operations and emergencies	H	H	H
	Exclusive use of frequencies or equivalent high priority access to other systems	H	H	H
Grade of service	Suitable grade of service	H	H	H
	Quality of service	H	H	H
	Reduced response times of accessing network and information directly at the scene of incidence, including fast subscriber/network authentication	H	H	H
Coverage	PPDR system should provide complete coverage within relevant jurisdiction and/or operation	H	H	M
	Coverage of relevant jurisdiction and/or operation of PPDR organization whether at national, provincial/state or at local level	H	H	M
	Systems designed for peak loads and wide fluctuations in use	H	H	M
	Enhancing system capacity during PP emergency or DR by techniques such as reconfiguration of networks with intensive use of direct mode operation	H	H	H
	Vehicular repeaters (NB, WB, BB) for coverage of localized areas	H	H	H
	Reliable indoor/outdoor coverage	H	H	H
	Coverage of remote areas, underground and inaccessible areas	H	H	H
	Appropriate redundancy to continue operations, when equipment/infrastructure fails	H	H	H
Capabilities	Rapid dynamic reconfiguration of system	H	H	H
	Control of communications including centralized dispatch, access control, dispatch (talk) group configuration, priority levels and pre-emption.	H	H	H
	Robust OAM offering status and dynamic reconfiguration	H	H	H
	Internet Protocol compatibility (complete system or interface with)	M	M	M

TABLE 3 (*cont.*)

Requirement	**Specifics**	**Importance(1)**		
		PP (1)	**PP (2)**	**DR**
Capabilities (*cont.*)	Robust equipment (hardware, software, operational and maintenance aspects)	H	H	H
	Portable equipment (equipment that can transmit while in motion)	H	H	H
	Equipment requiring special features such as high audio output, unique accessories (e.g. special microphones, operation while wearing gloves, operation in hostile environments and long battery life)	H	H	H
	Fast call set-up and instant push-to-talk operation	H	H	H
	Communications to aircraft and marine equipment, control of robotic devices	M	H	L
	One touch broadcasting/group call	H	H	H
	Terminal-to-terminal communications without infrastructure (e.g. direct mode operations/talk-around), vehicular repeaters	H	H	H
	Appropriate levels of interconnection to public telecommunication network(s)	M	M	M
2. *Security*	End-to-end encrypted communications for mobile-mobile, dispatch and/or group calls communications	H	H	L
3. *Cost related*	Open standards	H	H	H
	Cost effective solution and applications	H	H	H
	Competitive marketplace	H	H	H
	Reduction in deployment of permanent network infrastructure due to availability and commonality of equipment	H	H	L
4. *EMC*	PPDR systems operation in accordance with national EMC regulations	H	H	H
5. *Operational*				
Scenario	Support operation of PPDR communications in any environment	H	H	H
	Implementable by public and/or private operator for PPDR applications	H	H	M
	Robust OAM offering status and dynamic reconfiguration	H	H	H
	Rapid deployment of systems and equipment for large emergencies, public events and disasters (e.g. large fires, Olympics, peacekeeping)	H	H	H
	Information to flow to/from units in the field to the operational control center and specialist knowledge centers	H	H	H
	Greater safety of personnel through improved communications	H	H	H
Interoperability	Intra-system: Facilitate the use of common network channels and/or talkgroups	H	H	H
	Inter-system: Promote and facilitate the options common between systems	H	H	H
	Coordinate tactical communications between on-scene or incident commanders of the multiple PPDR agencies	H	H	H

TABLE 3 (*end*)

Requirement	Specifics	Importance(1)		
		PP (1)	**PP (2)**	**DR**
6. *Spectrum usage and management*	Share with other terrestrial mobile users	L	L	M
	Suitable spectrum availability (NB, WB, BB channels)	H	H	H
	Minimize interference to PPDR systems	H	H	H
	Efficient use of spectrum	M	M	M
	Appropriate channel spacing between mobile and base station frequencies	M	M	M
7. *Regulatory compliance*	Comply with relevant national regulations	H	H	H
	Coordination of frequencies in border areas	H	H	M
	Provide capability of PPDR system to support extended coverage into neighbouring country (subject to agreements)	M	M	M
	Ensure flexibility to use various types of systems in other Services (e.g. HF, satellites, amateur) at the scene of large emergency	M	H	H
	Adherence to principles of the Tampere Convention	L	L	H
8. *Planning*	Reduce reliance on dependencies (e.g. power supply, batteries, fuel, antennas, etc.)	H	H	H
	As required, have readily available equipment (inventoried or through facilitation of greater quantities of equipment)	H	H	H
	Provision to have national, state/provincial and local (e.g. municipal) systems	H	H	M
	Pre-coordination and pre-planning activities (e.g. specific channels identified for use during disaster relief operation, not on a permanent, exclusive basis, but on a priority basis during periods of need)	H	H	H
	Maintain accurate and detailed information so that PPDR users can access this information at the scene	M	M	M

(1) The importance of that particular requirement to PPDR is indicated as high (H), medium (M), or low (L). This importance factor is listed for the three radio operating environments: "Day-to-day operations", "Large emergency and/or public events", and "Disasters", represented by PP (1), PP (2) and DR, respectively.

Annex 3

Narrowband frequencies for inter-agency coordination and safety and security communications in international humanitarian assistance presently in use

The Working Group on Emergency Telecommunications (WGET), which is also the Reference Group on Telecommunications (RGT) of the Inter-Agency Standing Committee (IASC) on humanitarian affairs for the United Nations, has adopted and uses the following frequencies whenever the situation permits.

Within the spectrum allocated to land-mobile service in the VHF range:

Primary channel (A):

Simplex: 163.100 MHz

Duplex: Repeater transmits on 163.100 MHz
Repeater receives on 158.100 MHz

Alternative channel (B):

Simplex: 163.025 MHz

Duplex: Repeater transmits on 163.025 MHz
Repeater receives on 158.025 MHz

Alternative channel (C):

Simplex: 163.175 MHz

Duplex: Repeater transmits on 163.175 MHz
Repeater receives on 158.175 MHz

Within the spectrum allocated to land-mobile service in the UHF range:

Primary channel (UA):

Simplex: 463.100 MHz

Duplex: Repeater transmits on 463.100 MHz
Repeater receives on 458.100 MHz

Alternative channel (UB):

Simplex: 463.025 MHz

Duplex: Repeater transmits on 463.025 MHz
Repeater receives on 458.025 MHz

Alternative channel (UC):

Simplex: 463.175 MHz

Duplex: Repeater transmits on 463.175 MHz
Repeater receives on 458.175 MHz

Annex 4

Spectrum requirements for public protection and disaster relief

1 Introduction

This Annex addresses the estimation of the spectrum requirements for public protection and disaster relief (PPDR), particularly within the context of WRC-03 agenda Item 1.3. The Annex provides:

- a method of calculating amounts of spectrum;
- system scenarios and assumptions;
- validation of the method with respect to existing applications;
- examples of several administrations projections of their requirements by 2010;
- determining the amount of spectrum which should be harmonized in the context of future applications; and
- conclusions.

The calculation method given in this Annex is provided for assisting in consolidating spectrum requirements.

A number of administrations have used the modified methodology in Appendix 1 to this Annex to estimate their national spectrum requirements for PPDR. That methodology, however, is not the only means by which administrations may calculate their national PPDR spectrum needs. Administrations have the discretion to use whatever method, including the modified methodology; they choose to determine their own spectrum requirements for PPDR.

Many PPDR entities around the world are currently evaluating the migration from analog wireless systems to digital for current telecommunication services. The migration to digital will also allow these entities to add some advanced services to these first generation PPDR digital systems. However, there are many more advanced services that PPDR users are likely to demand as they become available to commercial users. While spectrum demand has been estimated and allotted for 2nd and 3rd generation commercial wireless services, similar analysis has not been done for PPDR users.

The greatest demand for public protection and disaster relief telecommunication services is in large cities where different categories of traffic can be found, i.e. that generated by mobile stations (MS), vehicle mounted or portable stations, and personal stations (PS) (hand-held portable radios). The trend is toward designing the PPDR telecommunication network to provide services to personal stations both outdoor and indoor (building penetration).

Maximum demand will be created after a disaster, when many PPDR users converge on the emergency scene utilizing existing telecommunication networks, installing temporary networks, or utilizing vehicle mounted or portable stations. Additional spectrum may be required for interoperability between various PPDR users and/or additional spectrum may be required for installation of temporary disaster relief systems.

Considerations on spectrum demand should take into account the estimated traffic, the available and foreseeable techniques, the propagation characteristics and the time-scale to meet the users' needs to the greatest possible extent. Consideration on frequency matters should take into account that the traffic generated by mobile systems, as well as the number and diversity of services, will continue to grow.

Any estimation of the traffic should take into consideration that in the future, non-voice traffic will constitute an increasing portion of the total traffic and that traffic will be generated indoors as well as outdoors by personal and mobile stations.

2 Methods of projecting spectrum requirements

2.1 Description of the methodology

This public protection and disaster relief spectrum calculation methodology (Appendix 1 to this Annex) follows the format of the generic methodology that was used for the calculation of IMT-2000 terrestrial spectrum requirements (Recommendation ITU-R M.1390). The use of the methodology can be customized to specific applications by selecting values appropriate to the particular terrestrial mobile application. Another model based on a generic city approach was also used (see Appendix 2 to this Annex)

The values selected for the PPDR applications must take into account the fact that PPDR utilizes different technologies and applications (including dispatch and direct mode).

2.2 Required input data

The ITU-R M.1390 based model and the generic city model require a number of input values which can be categorized as environment, traffic or network systems. In applying the model to PPDR the main data elements required are:

– the identification of PPDR user categories, e.g. police, fire, ambulance;
– the number of users in each category;
– the estimated number of each user category in use in the busy hour;
– the type of information transmitted, e.g. voice, status message and telemetry;
– the typical area to be covered by the system under study;
– the average cell size of base stations in the area;
– the frequency reuse pattern;
– the grade of service;
– the technology used including RF channel bandwidth;
– the demographic population of the city.

2.3 Validity of the methodology

2.3.1 Discussion

Several aspects of the methodology, the assumptions inherent in the model as presented, timing, method of calculation, frequency reuse, possibility of separating the calculations for PPDR, urban as opposed to rural situations, and the nature of the operating environments were clarified in the ITU-R study period 2000-2003.

Specifically, the following issues were raised in connection with the methodology:

a) Applicability of IMT-2000 methodology to PPDR?
b) Substituting the geographic areas (e.g. urban, in-building, etc.) in the IMT-2000 methodology by service categories (NB, WB, BB)?

c) Use of assumptions of PSWAC Report[4] with regard to assessment of traffic for PPDR?

d) Treatment of traffic for PP and DR together?

e) Use of cellular configurations/hotspots in estimating spectrum requirements for PPDR?

f) Applicability of the methodologies for the simplex/direct mode operations?

In response, the following points should be noted:

1 While the document is based on the methodology used for IMT-2000, the method is capable of including all technologies from simplex to cellular and beyond. Further work will be required to establish appropriate classifications of service environment categories (e.g. for fire, police, emergency medical services) and model systems for those environments, in order to make the calculations needed for each type of use and technology.

2 Terms of the calculation of spectrum requirements public protection activities could be separated from disaster relief activities, with separate and appropriate parameter values and assumptions being applied for each case. However, it was noted that there are instances where public protection equipment, which is used for routine operations on a day-by-day basis, may also be employed in times of disaster. In these cases, there would need to be some means established to avoid double counting when undertaking calculations of spectrum requirements.

3 In considering the service environments (i.e. narrowband, wideband and broadband), it was noted that those used for IMT-2000 may also have some applicability to PPDR communications.

2.3.2 Validity study

One administration undertook the performance of a study of the validity of the results predicted by this methodology. This was done by inputting the parameters of a working narrowband PPDR system into a calculator spreadsheet and checking that the amount of spectrum it predicted was the same as that actually used by the system. It was concluded that this methodology is valid, provided it is used carefully and correctly. It was also concluded that although not validated by actual measurement, one might extrapolate that model works as well for wideband and broadband as long as the input parameters are carefully considered and applied. Another administration reported on a similar study undertaken in which examples were developed for typical cities, obtaining spectrum estimates that are consistent with other examples previously reported. Using two examples of the application of the methodology – one referred to a middle-sized city and the other to an industrial district – it was concluded that the methodology is appropriate for the evaluation of spectrum needed for PPDR radiocommunication.

2.4 Critical parameters

In assessing the validity of the methodology several critical parameters were identified which must be selected with care. Studies in estimating spectrum requirements for terrestrial land mobile systems were conducted by some administrations showed that the most influential input parameters are:

– cell radius/frequency reuse;

– number of users.

---

[4] United States Public Safety Wireless Advisory Committee, Attachment D, Spectrum Requirements Subcommittee Report, September 1996.

The results of the studies were shown to be heavily dependent upon cellular architecture parameters. The studies show that changes in cell radius will change the spectrum estimate significantly. While it is true that reducing the size of the cell radius will increase the reuse of the spectrum and thereby reduce the spectrum requirement, the cost of the infrastructure will also significantly increase. Similar considerations apply to other parameters, e.g. using sectored cells decreases the necessary spectrum by a factor of three. For these reasons it is advisable that careful studies of cellular structures are undertaken prior to the final specification of the spectrum to be reserved to PPDR.

In preparing the estimate of spectrum amounts, it will be necessary to get consensus on the input data to put into the generic methodology. Noting the sensitivity of the results to such critical parameters, the input data will need to be selected carefully and will need to reflect a balance between the amount of spectrum sought and the infrastructure cost. Countries that need less spectrum than the full amount identified will have greater freedom in network design, the degree of frequency reuse and infrastructure cost.

2.5 Extrapolated upper limit

Korea undertook a parametric analysis of the result of spectrum calculations made for Bhopal, Mexico City, and Seoul. The analysis also used data for other cites taken from other contributions to the work of the ITU-R. The parametric analysis provided insight into PPDR spectrum requirements and it showed that considering the worst case/dense user situation a maximum of 200 MHz (Narrowband: 40 MHz, Wideband: 90 MHz, Broadband: 70 MHz) is needed for the PPDR spectrum requirement for WRC-03 Agenda Item 1.3.

3 Results

3.1 Results of estimates of amount of spectrum required by the year 2010 for PPDR

A summary of results of spectrum estimates for PPDR scenarios presented by some administrations using the proposed spectrum calculator methodology is given below. However the data in the last row was made using various other methods.

Location	Narrowband (MHz)	Wideband (MHz)	Broadband (MHz)	Total (MHz)
Delhi	51.8	3.4	47.6	102.8
Bhopal	24	5.2	32.2	61.4
Seoul	15.1	90.5	69.2	174.8
Mexico City	46.2	39.2	50.2	135.6
Paris	16.6	32.6	–	–
Medium city (Italy high penetration)	21.1	21.6	39.2	81.9
Medium city (Italy medium penetration)	11.6	11.4	39.2	62.2
Industrial district (Italy)	3.0	3.0	39.2	45.2
USA	35.2	12	50.0	97.2

The United States of America provided its current spectrum designations for PPDR and did not use the proposed methodology. It reported that it has designated a total of 35.2 MHz of spectrum for local and state PPDR agencies to use for narrowband applications. In addition, 12 MHz of spectrum has been designated for wideband PPDR applications. It has designated 50 MHz spectrum for broadband PPDR applications. The United States of America is continually reviewing its spectrum decisions to determine if spectrum has been designated appropriately for state and local PPDR applications.

3.2 Discussion of results

The totals listed in the above chart cover all the PPDR applications and both uplink and downlink requirements. The results range between 45 MHz and 175 MHz. Such results have to be compared with the national current and forecasted situations taking into account the whole spectrum needed by PPDR users.

There are several reasons for the wide range of spectrum estimates. First, the studies done in obtaining these results showed that the spectrum estimates are very dependent on density and the penetration rate. Second, administrations based their spectrum calculations on whatever scenarios they deemed most appropriate. For example, Korea based its spectrum calculations on the worst case/most dense user requirement. Italy chose to examine the PPDR spectrum needs of a typical medium-size city in Italy. Other administrations used other scenarios.

Many countries do not envisage having physically separate PP and DR networks in their countries and therefore see global/regional harmonization as applying to both PP and DR requirements. Other countries may decide to calculate separate PP and DR spectrum requirements.

Appendix 1
to Annex 4

Methodology for the calculation of public protection and disaster relief terrestrial spectrum requirements

1 Introduction

The function of this attachment is to present an initial forecast for spectrum needed by public protection and disaster relief (PPDR) by the year 2010. A spectrum calculator methodology, following the format of ITU methodology for the calculation of IMT-2000 spectrum requirements, is developed. Because of the differences between commercial wireless users and PPDR wireless users, alternate methodologies are proposed to calculate PPDR user penetration rates and define the PPDR operational environments. Methodologies are also proposed to define PPDR net system capacity and PPDR quality of service.

The analysis is based upon current PPDR wireless technologies and expected trends in demand for advanced applications. From that, an initial forecast can be made for the amount of spectrum needed for specific advanced telecommunication services through the year 2010.

2 Advanced services

The advanced services likely to be available to PPDR community by year 2010 are:

– voice dispatch;
– telephone interconnect;
– simple messages;
– transaction processing;
– simple images (facsimile, snapshot);
– remote file access for decision processing;
– Internet/intranet access;
– slow video;
– full motion video;
– multimedia services, like videoconference.

A Spectrum prediction model

This spectrum prediction model follows the methodology for the prediction of IMT-2000 Spectrum Requirements (Recommendation ITU-R M.1390).

The steps to be used are:

Step 1: Identify the geographical area over which the model will be applied.

Step 2: Identify the population of PPDR personnel.

Step 3: Identify the advanced services used by the PPDR community through year 2010.

Step 4: Quantify technical parameters that apply to each of the advanced services.

Step 5: Forecast the spectral need for each advanced service.

Step 6: Forecast total spectral need for PPDR through year 2010.

See Attachment A for a comparison of the proposed PPDR methodology versus the Recommendation ITU-R M.1390 methodology. See Attachment B for a flowchart of the proposed PPDR methodology.

B Geographical area

Determine the PPDR user populations within the area of the study.

For this model, we do not need to investigate spectrum demand over an entire country. The area(s) of interest will be one or more of the major metropolitan regions within each country. The population density is highest in these areas. The proportion of PPDR personnel relative to the general population is expected to be highest here, also. Therefore, the demand for spectrum resources should also be highest in the major metropolitan area(s). This is similar to the IMT-2000 methodology where the geography and environments of only the most significant contributors to spectrum requirements are considered.

We need to clearly define the geographic and/or political boundaries of the metropolitan area of study. This may be the political boundary of the city or of the city and surrounding suburban cities and/or counties in the metropolitan area. We need general population data for the metropolitan area. This should be readily available from census data.

Instead of using general population density (population/km^2), the PPDR population and penetration rates must be determined. Within the geopolitical boundaries of the study area, PPDR population must be defined and divided by the area to determine the PPDR user density (PPDR/km^2).

Representative cell area (radius, geometry) needs to be determined for each operational environment within the geographic study area. This is dependent upon the population density, network design, and network technology. PPDR networks tend to utilize higher power devices and larger radius cells than commercial systems.

Follow IMT-2000 methodology A:

Define geographic boundaries and area (km^2) of each environment.

C Operational environments versus service environments

In the methodology for the calculation of IMT-2000 spectrum requirements, the analysis is conducted on physical operational environments. These environments vary significantly in cell geometry and/or population density. PPDR population density is much lower than the general population density. PPDR networks generally provide wireless services into all physical environments from one, or more, wide-area network(s). This model defines "service environments" which group services by the type of PPDR wireless telecommunication network: narrowband, wideband and broadband. Many services are currently, and will continue to be, delivered by networks using narrowband channels (25 kHz or less). These include dispatch voice, transaction processing, and simple images. More advanced services like internet/intranet access and slow video will require a wideband channel (50 to 250 kHz) to deliver these higher content services. Full motion video and multi-media services will require very wide channels (1 to 10 MHz) to deliver real-time images. These three "service environments" are likely to be deployed as separate overlapping networks utilizing different cell geometries and different network and subscriber technologies.

Also, the services offered within each "service environment" will need to be defined.

Modified version of IMT-2000 methodology A1, A2, A3, A4, B1:

Define "service environment", i.ẹ. narrowband, wideband, broadband.

Determine direction of calculations for each environment: uplink, downlink, combined.

Determine average/typical cell geometry within each "service" environment.

Calculate representative cell area within each "service" environment.

Define services offered in each "service environment" and net user bit rate for each.

D PPDR population

Who are PPDR users? These are personnel who respond to day-to-day emergencies and to disasters. They would typically be public protection personnel grouped into mission oriented categories, such as police, fire brigades, emergency medical response. For disasters the scope of responders may increase to include other government personnel or civilians. All these PPDR personnel would be using PPDR telecommunication services during an emergency or disaster. PPDR users may be combined together into categories that have similar wireless communication usage patterns, i.e. the assumption is that all users grouped into "police" category personnel would have similar demands for telecommunication services.

For this model, the categories will only be used to group PPDR users with similar wireless service usage rates. That is, for police, each officer may have a radio, so the wireless penetration rate is 100% for police. For ambulance crews, there may be two people assigned to an ambulance, but only one radio, so the penetration rate is only 50% for ambulance crews. The current penetration rate can easily be determined if the number of mobile and portable stations deployed is known. It is simply the ratio of the number of radios deployed to the number of PPDR users in that category.

We need to determine the PPDR user populations. This can be collected for each PPDR user category; police, law enforcement, fire brigade, emergency medical response, etc. This data may be collected from the specific metropolitan governments or PPDR agencies. This data may be available from several public sources, including annual budgets, census data, and reports published by national or local law enforcements agencies.

The data may be presented in several formats, which must be converted into the total counts from each source for each PPDR category within the area of study.

– Some data may be presented as specific PPDR user counts within a political sub-division; e.g. city A with a population of nnnnn has AA police officers, BB fire fighters, CC ambulance drivers, DD transit police, EE traffic wardens, and FF civilian support personnel.

– Some data may be presented as a percentage relative to the total population; e.g. there are XXX police officers per 100 000 population. This needs to be multiplied by the population within the area of study to calculate the total count for each PPDR category.

– There may be multiple levels of government within the area of study. The PPDR totals for each category need to be combined. Local police, county police, state police, and federal police could be combined into a single "police" category. The assumption is that all these "police" category personnel would have similar demands for telecommunication services.

Example of PPDR categories:

Regular Police	Fire Brigades	Emergency Medical Services
Special Police Functions	Part-time Fire	EMS Civilian Support
Police Civilian Support	Fire Civilian Support	
General Government Personnel	Other PPDR Users	

Growth projections for population and planned increases in PPDR personnel may be used to estimate the future number of PPDR personnel within the area of study in 2010. Analysis over the study area may show that some towns/cities within the area of study do not provide advanced PPDR services today, but plan to deliver those services within the next 10 years. Growth projection may simply be the application of the higher PPDR user population density figures from cities/towns using advanced wireless services today within the area of study to all parts of the study area.

Modified version of IMT-2000 methodology B2:

Determine PPDR population density within study area.

– Calculate for each mission-oriented category of PPDR user or for groups of PPDR users with similar service usage patterns.

E Penetration rates

Instead of using penetration rates from commercial wireless market analyses, the PPDR penetration rates for current and future wireless telecommunication services must be determined. It is expected that the ITU-R survey on PPDR communications will supply some of this data. One method would be to determine the penetration rate of each telecommunication service within each of the PPDR categories defined above, then convert this to the composite PPDR penetration rate for each telecommunication service within each environment.

Modified version of IMT-2000 methodology B3, B4:

Calculate PPDR population density.

– Calculate for each category of PPDR user.

Determine penetration rate for each service within each environment.

Determine users/cell for each service within each environment.

F Traffic parameters

The proposed model follows the IMT-2000 methodology. Traffic parameters used in examples below represent average for all PPDR users. However, these traffic parameters could also be calculated for individual PPDR categories and combined to calculate composite traffic/user. Much of this data was determined by PSWAC and that busy hour traffic data will be used in the examples presented below. The "busy hour call attempts" are defined as the ratio between the total number of connected calls/sessions during the busy hour and the total number of PPDR users in the study area during the busy hour. Much of this data was determined by PSWAC and that busy hour traffic data will be used in the examples presented below. The activity factor is assumed to be 1 for all services, including PPDR speech. Current PPDR systems do not use vocoders with discontinuous voice transmission, so PPDR speech continuously occupies the channel and the PPDR speech activity factor is 1.

Follow IMT-2000 methodology B5, B6, B7:

Determine busy hour call attempts per PPDR user for each service in each environment.

Determine effective call/session duration.

Determine activity factor.

Calculate busy hour traffic per PPDR user.

Calculate offered traffic/cell (E) for each service in each environment.

Example of traffic profiles from PSWAC Report:

PSWAC traffic profile summary		Inbound (E)	Outbound (E)	Total (E)	(s)	Ratio of busy hour to average hour	Conti-nuous bit rate (at 4 800 bit/s)
Voice	Current busy hour	0.0073484	0.0462886	0.0536370	193.1	4.00	85.8
	Current average hour	0.0018371	0.0115722	0.0134093	48.3		21.5
	Future busy hour	0.0077384	0.0463105	0.0540489	194.6	4.03	86.5
	Future average hour	0.0018321	0.0115776	0.0134097	48.3		21.5
Data	Current busy hour	0.0004856	0.0013018	0.0017874	6.4	4.00	2.9
	Current average hour	0.0001214	0.0003254	0.0004468	1.6		0.7
	Future busy hour	0.0030201	0.0057000	0.0087201	31.4	4.00	14.0
	Future average hour	0.0007550	0.0014250	0.0021800	7.8		3.5
Status	Current busy hour	0.0000357	0.0000232	0.0000589	0.2	4.01	0.1
	Current average hour	0.0000089	0.0000058	0.0000147	0.1		0.0
	Future busy hour	0.0001540	0.0002223	0.0003763	1.4	3.96	0.6
	Future average hour	0.00	0.00	0.00	0.34		0.15
Image	Current busy hour	0.0268314	0.0266667	0.0534981	192.6	4.00	85.6
	Current average hour	0.0067078	0.0066670	0.0133748	48.1		21.4

G PPDR quality of service functions

The IMT-2000 methodology takes the offered traffic/cell data, converts it to the number of traffic channels required to carry that load in a typical cell reuse grouping, and then applies grade of service formulas to determine the number of service channels needed in a typical cell. The same methodology is proposed here, but the factors used for PPDR networks are significantly different.

For PPDR systems the reuse pattern is typically much higher than commercial wireless services. Commercial wireless services are normally designed to use low power devices with power control in an interference limited environment. PPDR systems are typically designed to be "coverage" or "noise" limited. Many PPDR systems use a mixture of high power vehicular devices and low power handheld devices, without power control. Therefore, the separation or reuse distance is much greater for PPDR systems, in the range of 12 to 21.

The technology modularity of PPDR systems is often different than commercial systems. There may be two or more networks covering the same geographic area, in different frequency bands, supporting the PPDR personnel from different levels of government or in different PPDR categories (federal networks may be independent of local networks; police networks may be independent of fire networks). The result is networks with fewer channel resources per cell.

PPDR networks are normally designed for higher coverage reliabilities, 95 to 97%, because they are trying to cover all operational environments from a fixed network. Commercial networks, with a revenue stream, can continuously adapt their networks to changing user needs. PPDR networks, funded with public monies, normally undergo minimal change in cell locations or service channels per cell over their lifetime of 10-20 years.

For PPDR services, availability of the channel must be very high, even during busy hours, because of the immediate need to transmit critical, sometimes life-saving, information. PPDR networks are designed for lower call blocking levels, <1%, as PPDR personnel need immediate access to the network during emergency situations. While many routine conversations and data transactions can wait several seconds for a response, many PPDR situations are highly tense and require immediate channel availability and response.

Loading varies greatly for different PPDR network topologies and for different PPDR situations. Many police or fire situations may require individual channels to be set aside for on-scene interoperability with very low loading, <10%. Conventional, single channel, mobile relay systems in use today typically operate at 20-25% loading, because unacceptable blockage occurs at higher loading. Large 20 channel trunked systems, which spread the load across all available channels, with a mix of critical and non-critical users, may be able to operate at acceptable levels for critical PPDR operations with busy hour loading of 70-80%.

The net impact causes the Erlang B factor for the average PPDR network to be higher, about 1.5, instead of the 1.1 to 1.2 factors seen with commercial services at 90% coverage and 1% blocking.

Follow IMT-2000 methodology B8:

Unique PPDR requirements:

Blocking = <1%

Modularity = ~ 20 channels per cell per network, results in a high Erlang B factor of about 1.5.

Frequency reuse cell format

– 12 for like power mobile or personal stations

– 21 for mixture of high/low power mobile and personal stations.

Determine number of service channels needed for each service in each "service" environment (NB, WB, BB)

H Calculate total traffic

The proposed model follows the IMT-2000 methodology. The PPDR net user bit rate should include the raw data rate, the overhead factor and the coding factor. This is dependent upon the technology chosen for each service.

Information is coded to reduce or compress the content which minimizes the amount of data to be transmitted over an RF channel. Voice, which may be coded at a rate of 64 kbit/s or 32 kbit/s for wireline applications, is coded at rates of less than 4 800 bit/s for PPDR dispatch speech applications. The more the information is compressed, the more important each bit becomes, and the more important the error correction function becomes. Error coding rates from 50% to 100% of information content are typical. Higher transmission rates over the harsh multi-path propagation environment of an RF channel require additional synchronization and equalization functions, which use additional capacity. Also, other network access and control functions need to be carried along with the information payload (unit identity, network access functions, encryption).

PPDR systems in operation today use 50-55% of the transmitted bit rate for error correction and overhead.

For example: a technology for speech on narrowband channels may have a speech vocoder output rate of 4.8 kbit/s with a forward error correction (FEC) rate of 2.4 kbit/s and the protocol may be provisioned for another 2.4 kbit/s of overhead signalling and information bits, for a net user bit rate of 9.6 kbit/s.

Follow IMT-2000 methodology C1, C2, C3:

Define net user bit rate, overhead factors, coding factors for each service in each “service” environment.

Convert service channels from B8 back to per cell basis.

Calculate total traffic (Mbit/s) for each service in each “service” environment

I Net system capacity

The net system capacity is an important measure of the spectrum efficiency of a wireless telecommunications system. The net system capacity calculation produces the maximum system capacity possible within the spectrum band being studied.

The proposed model follows the IMT-2000 methodology. However, the calculation of PPDR net system capacity should be based upon typical PPDR technologies, PPDR frequency bands, and PPDR reuse patterns, rather than the GSM model used in the IMT-2000 methodology.

Attachment C provides an analysis for several PPDR technologies currently in use against some existing PPDR spectrum allocations. These examples show maximum possible system capacity for the purpose of estimating future spectrum requirements. There are numerous other user requirements and spectrum allocation factors, not included here, that affect the functional and operational deployment of a network, the choice of technology, and the resulting network’s spectrum efficiency.

Follow IMT-2000 methodology C4, C5:

Pick several PPDR network technologies.

Pick several representative frequency bands.

Follow same calculations format as GSM model.

Calculate typical net system capacities for PPDR land mobile radio technology.

J Spectrum calculations

The proposed model follows the IMT-2000 methodology.

PPDR networks are very likely to have coincident busy hours. Therefore the alpha factor will be 1.0.

The number of PPDR personnel is likely to grow with general population growth. The demand for PPDR services is likely to increase following trends similar to the demand for commercial wireless telecommunication services.

The beta factor can be set to a number greater than 1.0 here, or the growth factor can be included in the net system capacity calculations.

Follow IMT-2000 methodology D1, D2, D3, D4, D5, D6:

Define alpha factor = 1.

Define beta factor = 1 (include growth under net system capacity, ignore other outside effects for example calculations).

Calculate spectrum need for each service in each “service” environment.

Sum up spectrum needs for each “service” environment (NB, WB, BB).

Sum up total spectrum need.

Examples

See Attachment E for a detailed narrowband voice example using London data from Attachment D. Attachment F shows example calculation summaries for narrowband voice, message, and image for London and New York City and for wideband data and slow video for New York City.

Conclusion

It has been demonstrated that the IMT-2000 methodology (Recommendation ITU-R M.1390) may be adapted to calculate the system requirements for public protection and disaster relief communications (or applications). Methods have been provided to determine the PPDR user population and service penetration rates. “Service” environments have been defined over which PPDR spectrum requirements can be calculated. The factors necessary to adapt the IMT-2000 methodology to a PPDR methodology have been identified, including the development of a methodology to define PPDR net system capacity.

Attachment A
of Appendix 1 to Annex 4

Comparison of proposed methodology for the calculation of PPDR spectrum requirements to IMT-2000 methodology

IMT-2000 methodology (Recommendation ITU-R M.1390)	IMT-2000 methodology	Proposed PPDR methodology
A Geography		
A1 Operational Environment Combination of user mobility and user mobility. Usually only analyse most significant contributors.	**A1** Look at three physical environments with different user densities: urban area and in-building, pedestrian, vehicular users	**A1** PPDR user density is much lower and more uniform. PPDR users roam from one environment to another as they respond to emergencies. PPDR systems are usually designed to cover all environments (i.e., wide-area network provides in-building coverage). Instead of analyzing by physical environment, assume that there will likely be multiple overlapping systems each providing different services (narrowband, wideband, and broadband). Each service environment will probably operate in a different frequency band with different network architectures. Analyse three overlapping urban “service environments”: narrowband, wideband, broadband.
A2 Direction of calculation	**A2** Usually separate calculations for uplink and downlink due to asymmetry in some services	**A2** Same
A3 Representative cell area and geometry for each environment type	**A3** Average cell radius of radius to vertex for hexagonal cells	**A3** Same
A4 Calculate area of typical cell	**A4** Omni cells = πi R^2 Hexagonal cells = 2.6 · R^2 3-sector hex = 2.6/3 · R^2	**A4** Same

IMT-2000 methodology (Recommendation ITU-R M.1390)	**IMT-2000 methodology**	**Proposed PPDR methodology**
B Market & traffic		
B1 Services offered	**B1** Net user bit rate (kbit/s) For each service: speech, circuit data, simple messages, medium multimedia, high multimedia, highly interactive multimedia	**B1** Net user bit rate (kbit/s) for each of the three PPDR service environments: narrowband, wideband, broadband
B2 Population density Persons per unit of area within each environment. Population density varies with mobility	**B2** Potential users per km^2 Relative to general population	**B2** Total PPDR user population within the total area under consideration. Divide PPDR population by total area to get PPDR population density. PPDR users are usually separated into well-defined categories by mission. Example: *Category* — *Population* Regular Police — 25 498 Special Police Functions — 6 010 Police Civilian Support — 13 987 Fire Suppression — 7 081 Part-time Fire — 2 127 Fire Civilian Support — 0 Emergency Medical Services — 0 EMS Civilian Support — 0 General Government Services — 0 Other PPDR Users — 0 **Total PPDR population — 54 703** Area under consideration. Area within well-defined geographic or political boundaries. Example: City of London = 1 620 km^2 PPDR population density = PPDR population/area Example: London = 33.8 PPDR/km^2

<table>
<tr><th>IMT-2000 methodology
(Recommendation ITU-R M.1390)</th><th>IMT-2000 methodology</th><th>Proposed PPDR methodology</th></tr>
<tr>
<td>B3 Penetration rate

Percentage of persons subscribing to a service within an environment. Person may subscribe to more than one service</td>
<td>B3 Usually shown as table,

Rows are services defined in B1, such as speech, circuit data, simple messages, medium multi-media, high multimedia, highly interactive multimedia.

Columns are environments, such as in-building, pedestrian, vehicular</td>
<td>B3 Similar table.

Rows are services, such as voice, data, video

Columns are “service environments”, such as narrowband, wideband, broadband.

May collect penetration rate into each “service environment” separately for each PPDR category and then calculate composite PPDR penetration rate.

Example:
<table>
<tr><th>Category</th><th>Population</th><th>Penetration
(NB Voice)</th></tr>
<tr><td>Regular Police</td><td>25 498</td><td>100%</td></tr>
<tr><td>Special Police Functions</td><td>6 010</td><td>10%</td></tr>
<tr><td>Police Civilian Support</td><td>13 987</td><td>10%</td></tr>
<tr><td>Fire Suppression</td><td>7 081</td><td>70%</td></tr>
<tr><td>Part-time Fire</td><td>2 127</td><td>10%</td></tr>
<tr><td>Fire Civilian Support</td><td>0</td><td>0</td></tr>
<tr><td>Emergency Medical Services</td><td>0</td><td>0</td></tr>
<tr><td>EMS Civilian Support</td><td>0</td><td>0</td></tr>
<tr><td>General Government Services</td><td>0</td><td>0</td></tr>
<tr><td>Other PPDR Users</td><td>0</td><td>0</td></tr>
<tr><td>TOTAL PPDR Population</td><td>54 703</td><td></td></tr>
<tr><td>Narrowband Voice
PPDR Population</td><td>32 667</td><td></td></tr>
</table>
PPDR penetration rate for narrowband “service environment” and voice “service”: = Sum(Pop × Pen)/sum(Pop) = 59.7%</td>
</tr>
</table>

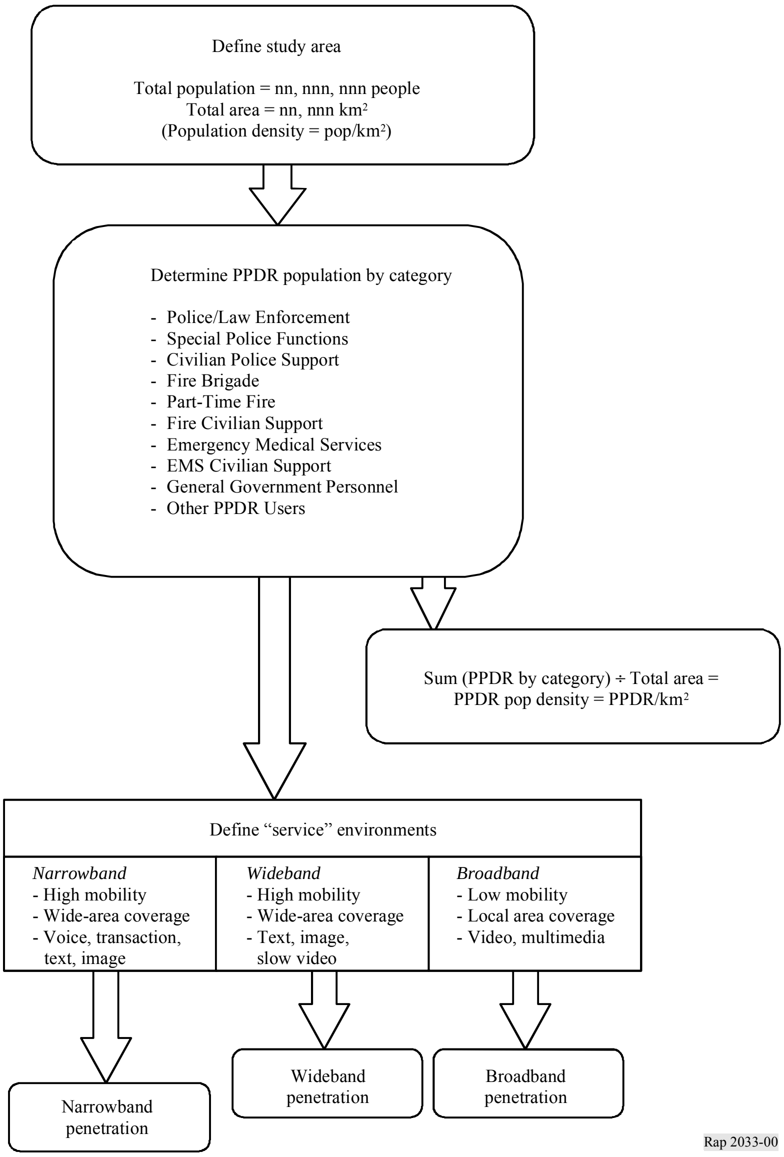
IMT-2000 methodology (Recommendation ITU-R M.1390)	IMT-2000 methodology	Proposed PPDR methodology
B4 Users/cell Number of people subscribing to service within cell in environment	**B4** Users/cell = Pop density × Pen Rate × Cell area	**B4** Same
B5 Traffic parameters Busy hour call attempts: average number of calls/sessions attempted to/from average user during a busy hour Effective call duration Average call/session duration during busy hour Activity factor Percentage of time that resource is actually used during a call/session. *Example*: bursty packet data may not use channel during entire session. If voice vocoder does not transmit data during voice pauses	**B5** Calls/busy hour s/call 0-100%	**B5** Same Sources: PSWAC Report or data collected from existing PPDR systems Same Same More likely that activity factor is 100% for most PPDR services.
B6 Traffic/user Average traffic generated by each user during busy hour	**B6** Call-seconds/user = Busy hour attempts × Call duration × Activity factor	**B6** Same
B7 Offered traffic/cell Average traffic generated by all users within a cell during the busy hour (3 600 s)	**B7** Erlangs = Traffic/user × User/cell/3 600	**B7** Same

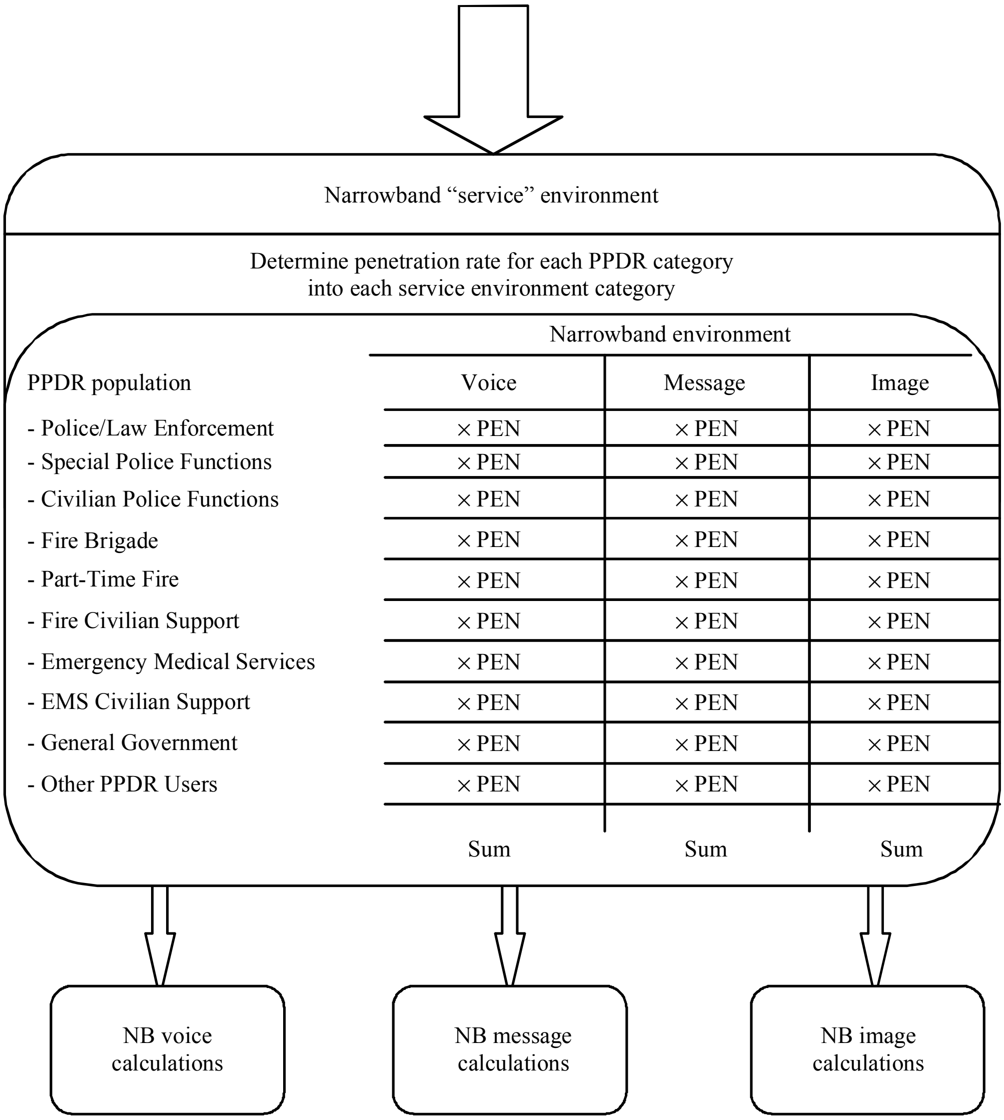
IMT-2000 methodology (Recommendation ITU-R M.1390)	IMT-2000 methodology	Proposed PPDR methodology
B8 Quality of service function Offered traffic/cell is multiplied by typical frequency reuse cell grouping size and quality of Service factors (blocking function) to estimate offered traffic/cell at a given quality level		
Group size	Typical cellular reuse = 7	Use 12 for portable only or mobile only systems. Use 21 for mixed portable and mobile systems. In mixed systems, assume that system is designed for portable coverage. Higher power mobiles in distant cells are likely to, so group size is increased from 12 to 21 to provide more separation.
Traffic per group	= Traffic/cell (E) × Group Size	Same
Service channels per group	Apply grade of service formulas Circuit = Erlang B with 1% or 2% blocking Packet = Erlang C with 1% or 2% delayed and delay/holding time ratio = 0.5	Similar Use 1% blocking. Erlang B factor probably close to 1.5. Need to consider extra reliability for PPDR systems, excess capacity for peak emergencies, and number of channels likely to be deployed at each PPDR antenna site. Technology modularity may affect number of channels that can be deployed at a site
C Technical and system considerations		
C1 Service channels per cell to carry offered load	**C1** Service channels per cell = Service channels per group/Group size	**C1** Same

IMT-2000 methodology (Recommendation ITU-R M.1390)	**IMT-2000 methodology**	**Proposed PPDR methodology**
C2 Service channel bit rate (kbit/s) Equals net user bit rate plus additional increase in loading due to coding and/or overhead signalling, if not already included	**C2** Service channel bit rate = Net user bit rate × Overhead factor × Coding factor If coding and overhead already included in Net user bit rate, then Coding factor = 1 and Overhead factor = 1	**C2** Same Can also sum effects of coding and overhead. If vocoder output = 4.8 kbit/s, FEC = 2.4 kbit/s, and Overhead = 2.4 kbit/s, then Channel bit rate = 9.6 kbit/s
C3 Calculate traffic (Mbit/s) Total traffic transmitted within area under study, including all factors	**C3** Total traffic = Service channels per cell x service channel bit rate	**C3** Same
C4 Net system capability Measure of system capacity for a specific technology. Related to spectral efficiency	**C4** Calculate for GSM system	**C4** Calculate for typical narrowband, wideband and broadband land mobile systems
C5 Calculate for GSM model 200 kHz channel bandwidth, 9 cell reuse, 8 traffic slots per carrier, frequency division duplex (FDD) with 2 × 5.8 MHz, 2 guard channels, 13 kbit/s in each traffic slot, 1.75 overhead/coding factor	**C5** Net system capacity for GSM model = 0.1 Mbit/s/MHz/cell	**C5** See Attachment A for several land mobile examples
D Spectrum Results		
D1-D4 Calculate individual components (each cell in service vs environment matrix)	**D1-D4** Freq = Traffic net system capacity for each service in each environment	**D1-D4** Similar, calculate for each cell in service vs. "service environment" matrix
D5 Weighting factor (alpha) for busy hour of each environment relative to busy hour of other environments, may vary from 0 to 1	**D5** if all environments have coincident busy hours, then alpha = 1 $Freq_{es}$ = Freq × alpha requirements in D1-D4	**D5** Same Same
D6 Adjustment factor (beta) for outside effects – multiple operators/networks, guard bands, band sharing, technology modularity	**D6** Freq(total) = beta × sum(alpha × $Freq_{es}$)	**D6** Same

Attachment B
of Appendix 1 to Annex 4

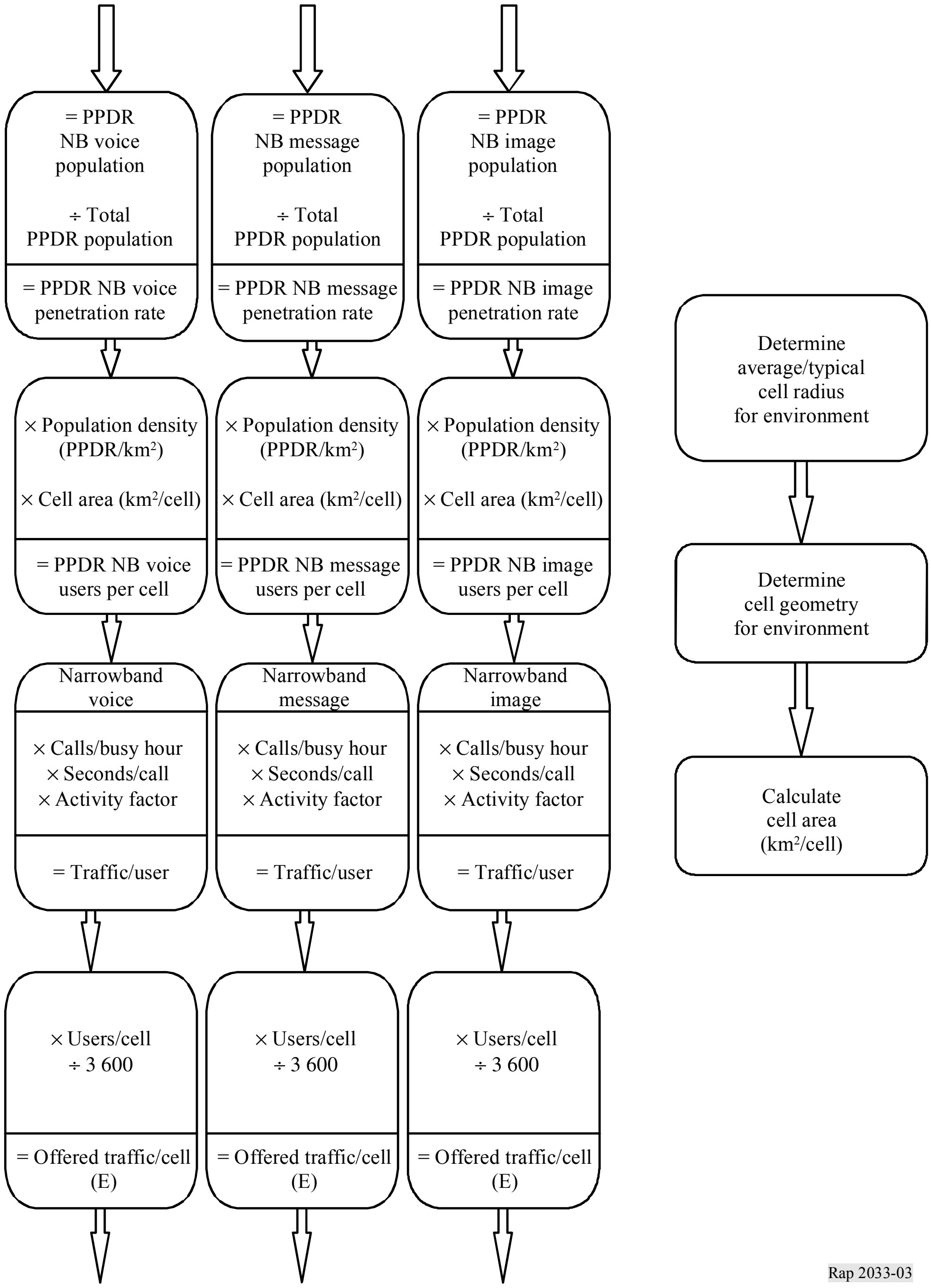
PPDR Spectrum Requirements Flowchart



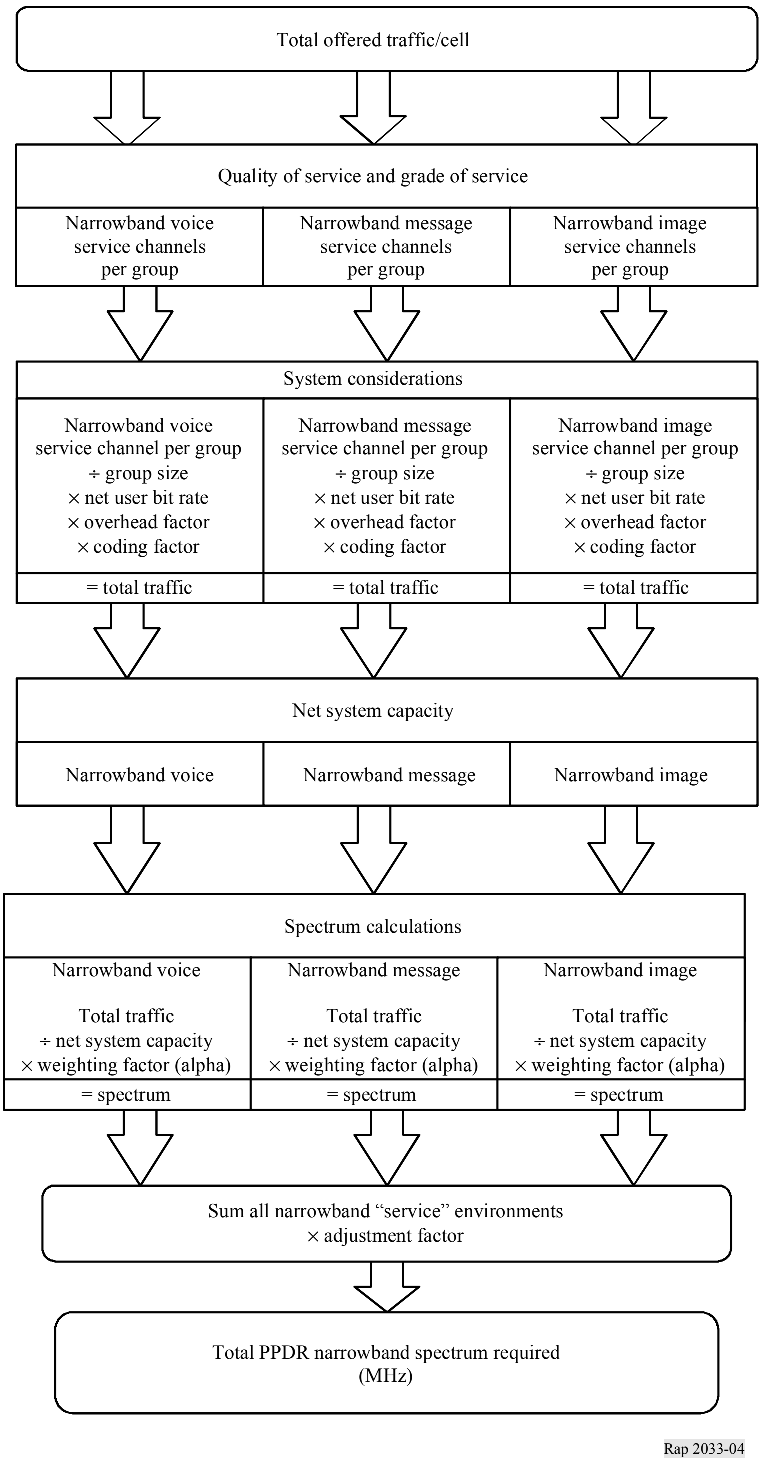


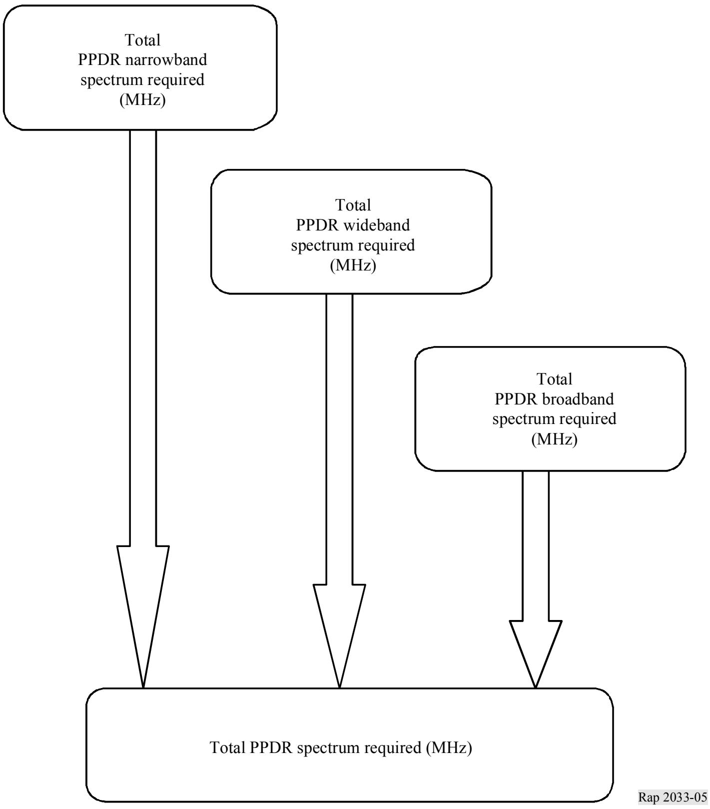
PEN: penetration

Rap 2033-02


= PPDR NB voice population
÷ Total PPDR population
= PPDR NB voice penetration rate
= PPDR NB message population
÷ Total PPDR population
= PPDR NB message penetration rate
= PPDR NB image population
÷ Total PPDR population
= PPDR NB image penetration rate
Determine average/typical cell radius for environment
× Population density (PPDR/km²)
× Cell area (km²/cell)
= PPDR NB voice users per cell
= PPDR NB message users per cell
= PPDR NB image users per cell
Determine cell geometry for environment
Narrowband voice
Narrowband message
Narrowband image
× Calls/busy hour
× Seconds/call
× Activity factor
= Traffic/user
Calculate cell area (km²/cell)
× Users/cell
÷ 3 600
= Offered traffic/cell (E)

Rap 2033-03


Total offered traffic/cell
Quality of service and grade of service
Narrowband voice service channels per group
Narrowband message service channels per group
Narrowband image service channels per group
System considerations
Narrowband voice service channel per group ÷ group size × net user bit rate × overhead factor × coding factor
Narrowband message service channel per group ÷ group size × net user bit rate × overhead factor × coding factor
Narrowband image service channel per group ÷ group size × net user bit rate × overhead factor × coding factor
= total traffic
= total traffic
= total traffic
Net system capacity
Narrowband voice
Narrowband message
Narrowband image
Spectrum calculations
Narrowband voice
Total traffic ÷ net system capacity × weighting factor (alpha)
Narrowband message
Total traffic ÷ net system capacity × weighting factor (alpha)
Narrowband image
Total traffic ÷ net system capacity × weighting factor (alpha)
= spectrum
= spectrum
= spectrum
Sum all narrowband "service" environments × adjustment factor
Total PPDR narrowband spectrum required (MHz)
Rap 2033-04



Attachment C
to Appendix 1 to Annex 4

System capacity calculation examples

1 IMT-2000 net system capacity calculation methodology

The spectrum efficiency factor is an important measure of the capacity of a wireless telecommunications system. In order compare spectrum efficiency factors it is necessary to use a common basis to calculate the system capacity (kbit/s/MHz/cell), available to carry traffic. Analysis should take into consideration factors which reduce capacity over the air interface (guard bands, co-channel and adjacent channel interference, channels assigned to other purposes within the band). This calculation should produce the maximum system capacity possible within the spectrum band being studied. Actual systems will be sized for lower traffic levels to achieve the desired grade of service.

Annex 3 of the SAG Report on UMTS/IMT-2000 Spectrum[5] calculates the capacity of a generalized GSM network as:

C4 and C5 Net system capability calculation

GSM and IMT-2000			
Width of band (MHz)	5.8	11.6	MHz total
Width of channel	0.2		MHz
		29.0	FDD channels within band
Reuse group factor	9		
		3.2	Channels per cell
Guard channels	2		(At band edge)
I/O channels	0		
		27.0	**Traffic channels**
Traffic/channel	8		8 TDMA slots per channel
Data/channel	13		kbit/s/slot
Overhead and signalling	1.75		(182 kbit/s per channel total)
		546.0	**kbit/s/cell**
		5.8	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		94.1	kbit/s/cell/MHz on outbound or inbound channel
Speech improvement	1.05	**98.8**	**kbit/s/cell/MHz on inbound or outbound channel with speech improvement**
All improvements	1.1	103.6	kbit/s/cell/MHz on outbound or inbound channel with all improvements

TDMA: time division multiple access.

The GSM net system capacity is usually rounded to 0.10 Mbit/s/MHz/cell for use in IMT-2000 calculations.

The same methodology is applied below to several example narrowband technologies and several sample spectrum bands. The examples show that the spectrum band structure and frequency reuse factor have a significant effect on the capacity calculation.

These are not meant to be a direct comparison between the selected technologies. There are numerous other user needs and spectrum allocation factors that effect the functional and operational deployment of a network, the choice of technology, and overall network efficiency. Some of the spectrum factors are considered in the alpha and beta factors (Recommendation ITU-R M.1390, D5 and D6).

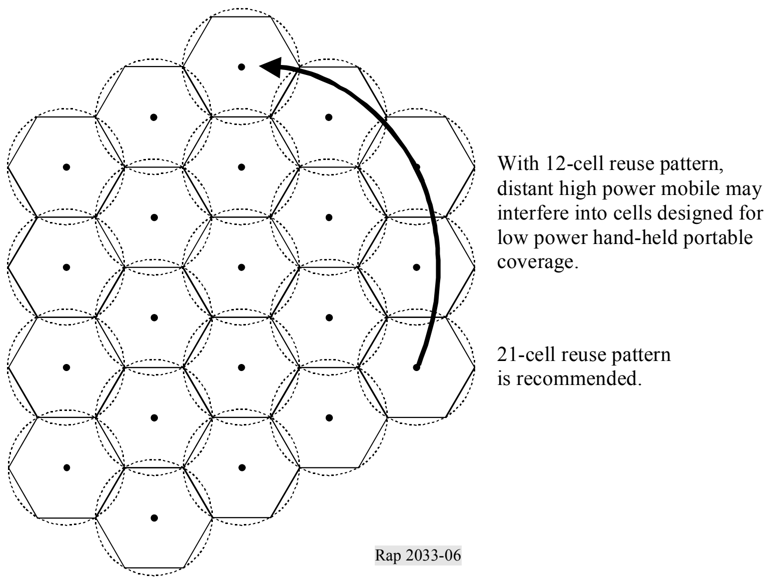
[5] UMTS Auction Consultative Group, A note on spectrum efficiency factors – UACG(98) 23. (http://www.spectrumauctions.gov.uk/documents/uacg23.html) Reference 1 = SAG Report, Spectrum calculations for terrestrial UMTS, release 1.2, 12 March 1998.

Net system capability summary

Spectrum band	Technology	Channels	Total capacity available
Reuse group factor = 12			
United States of America 821-824/866-869 MHz band	P25 phase I FDMA	1 × 12.5 kHz	60.0 kbit/s/MHz/cell
United States of America 700 MHz public safety band	P25 phase I FDMA	1 × 12.5 kHz	53.9 kbit/s/MHz/cell
United States of America 700 MHz public safety band	P25 phase II FDMA	1 × 6.25 kHz	107.7 kbit/s/MHz/cell
European 400 MHz public safety band	TETRA TDMA	4 slots/25 kHz	98.0 kbit/s/MHz/cell
Reuse group factor = 21			
United States of America 821-824/866-869 MHz band	P25 Phase I FDMA	1 × 12.5 kHz	34.3 kbit/s/MHz/cell
United States of America 700 MHz public safety band	P25 Phase I FDMA	1 × 12.5 kHz	30.8 kbit/s/MHz/cell
United States of America 700 MHz public safety band	P25 Phase II FDMA	1 × 6.25 kHz	61.6 kbit/s/MHz/cell
European 400 MHz public safety band	TETRA TDMA	4 slots/25 kHz	56.0 kbit/s/MHz/cell

FDMA: frequency division multiple access.

NOTE – 1 Reuse group factor of 12 is used for systems implementing only low power, handheld, portable devices. Reuse factor of 21 is used for systems implementing both handheld portables and higher power, vehicular mounted, mobile devices. Greater reuse factor is required because of potential for interference from distant mobiles into cells designed for portable coverage.



Example 1: Narrowband technologies for dispatch voice and low rate data.

Project 25 phase I, FDMA applied to United States of America 800 MHz public safety band.

C4 and C5 Net system capability calculation

NPSPAC using P25 phase I FDMA			**United States of America 821-824/866-869 MHz band**
Width of band (MHz)	3	6.0	MHz total
Width of channel	0.0125		
		240.0	FDD channels within band
Reuse group factor	12		(Portables only)
		20.0	Channels per cell
Guard channels	0		(At band edge)
I/O channels	15		(5 × 12.5 plus 12.5 kHz guard on each side of I/O channel)
		225.0	**Traffic channels**
Traffic/channel	1		
Data/channel	4.8		kbit/s
Overhead and signalling	2		(9.6 kbit/s per channel total)
		180.0	**kbit/s/cell**
		3.0	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		60.0	**kbit/s/cell/MHz on outbound or inbound channel**
Speech improvement	1.05	63.0	kbit/s/cell/MHz on outbound or inbound channel with speech improvement
All improvements	1.1	66.0	kbit/s/cell/MHz on outbound or inbound channel with all improvements

NPSPAC using P25 phase I FDMA			**United States of America 821-824/866-869 MHz band**
Width of band (MHz)	3	6.0	MHz total
Width of channel	0.0125		
		240.0	FDD channels within band
Reuse group factor	21		(Portables and mobiles)
		11.4	Channels per cell
Guard channels	0		(At band edge)
I/O channels	15		(5 × 12.5 plus 12.5 kHz guard on each side of I/O channel)
		225.0	**Traffic channels**
Traffic/channel	1		
Data/channel	4.8		kbit/s
Overhead and signalling	2		(9.6 kbit/s per channel total)
		102.9	**kbit/s/cell**
		3.0	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		34.3	**kbit/s/cell/MHz on outbound or inbound channel**
Speech improvement	1.05	36.0	kbit/s/cell/MHz on outbound or inbound channel with speech improvement
All improvements	1.1	37.0	kbit/s/cell/MHz on outbound or inbound channel with all improvements

Example 2: Narrowband technologies for dispatch voice and low rate data.

Project 25 Phase I, FDMA applied to United States of America 700 MHz public safety band.

C4 and C5 Net system capability calculation

P25, Phase I FDMA			**United States of America 700 MHz public safety band**
Width of band (MHz)	6	12.0	MHz total (4 × 3 MHz blocks)
Width of channel	0.0125		
		480.0	FDD channels within band
Reuse group factor	12		(Portables only)
		40.0	Channels per cell
Guard channels	12		(Low power channels at band edge)
I/O channels	64		(32 × 12.5 kHz I/O plus 32 × 12.5 kHz reserve)
		404.0	**Traffic channels**
Traffic/channel	1		
Data/channel	4.8		kbit/s
Overhead and signalling	2		(9.6 kbit/s per channel total)
		323.2	**kbit/s/cell**
		6.0	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		53.9	**kbit/s/cell/MHz on outbound or inbound channel**
Speech improvement	1.05	56.6	kbit/s/cell/MHz on outbound or inbound channel with speech improvement
All improvements	1.1	59.3	kbit/s/cell/MHz on outbound or inbound channel with all improvement

P25, Phase I FDMA			**United States of America 700 MHz public safety band**
Width of band (MHz)	6	12.0	MHz total (4 × 3 MHz blocks)
Width of channel	0.0125		
		480.0	FDD channels within band
Reuse group factor	21		(Portables and mobiles)
		22.9	Channels per cell
Guard channels	12		(Low power channels at band edge)
I/O channels	64		(32 × 12.5 kHz I/O plus 32 × 12.5 kHz reserve)
		404.0	**Traffic channels**
Traffic/channel	1		
Data/channel	4.8		kbit/s
Overhead and signalling	2		(9.6 kbit/s per channel total)
		184.7	**kbit/s/cell**
		6.0	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		30.8	**kbit/s/cell/MHz on outbound or inbound channel**
Speech improvement	1.05	32.3	kbit/s/cell/MHz on outbound or inbound channel with speech improvement
All improvements	1.1	33.9	kbit/s/cell/MHz on outbound or inbound channel with all improvements

Example 3: Narrowband technologies for dispatch voice and low rate data.

Project 25 phase II, FDMA applied to United States of America 700 MHz public safety band.

C4 and C5 Net system capability calculation

P25, Phase II FDMA			**United States of America 700 MHz public safety band**
Width of band (MHz)	6	12.0	MHz total
Width of channel	0.00625		
		960.0	FDD channels within band
Reuse group factor	12		(Portables only)
		80.0	Channels per cell
Guard channels	24		(Low power channels at band edge)
I/O channels	128		(64 × 6.25 kHz I/O plus 64 × 6.25 kHz reserve)
		808.0	**Traffic channels**
Traffic/channel	1		
Data/channel	4.8		kbit/s
Overhead and signalling	2		(9.6 kbit/s per channel total)
		646.4	**kbit/s/cell**
		6.0	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		107.7	**kbit/s/cell/MHz on outbound or inbound channel**
Speech improvement	1.05	113.1	kbit/s/cell/MHz on outbound or inbound channel with speech improvement
All improvements	1.1	118.5	kbit/s/cell/MHz on outbound or inbound channel with all improvements

P25, Phase II FDMA			**United States of America 700 MHz public safety band**
Width of band (MHz)	6	12.0	MHz total
Width of channel	0.00625		
		960.0	FDD channels within band
Reuse group factor	21		(Portables only)
		45.7	Channels per cell
Guard channels	24		(Low power channels at band edge)
I/O channels	128		(64 × 6.25 kHz I/O plus 64 × 6.25 kHz reserve)
		808.0	**Traffic channels**
Traffic/channel	1		
Data/channel	4.8		kbit/s
Overhead and signalling	2		(9.6 kbit/s per channel total)
		369.4	**kbit/s/cell**
		6.0	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		61.6	**kbit/s/cell/MHz on outbound or inbound channel**
Speech improvement	1.05	64.6	kbit/s/cell/MHz on outbound or inbound channel with speech improvement
All improvements	1.1	67.7	kbit/s/cell/MHz on outbound or inbound channel with all improvements

Example 4: Narrowband technologies for dispatch voice and low rate data.

TETRA TDMA applied to European 400 MHz public safety band.

C4 and C5 Net system capability calculation

TETRA TDMA			European 400 MHz public safety band
Width of band (MHz)	3	6.0	MHz total
Width of channel	0.025		
		120.0	FDD channels within band
Reuse group factor	12		(Hand-held portables only)
		10.0	Channels per cell
Guard channels	2		(At band edge)
Interoperability channels	20		(Reserve for direct mode operations)
		98.0	**Traffic channels**
Traffic/channel	4		Slots/channel
Data/channel	7.2		kbit/s/slot
Overhead and signalling	1.25		(36 kbit/s per channel total)
		294.0	**kbit/s/cell**
		3.0	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		98.0	**kbit/s/cell/MHz on outbound or inbound channel**
Speech improvement	1.05	102.9	kbit/s/cell/MHz on outbound or inbound channel with speech improvement
All improvements	1.1	107.8	kbit/s/cell/MHz on outbound or inbound channel with all improvements

TETRA TDMA			European 400 MHz public safety band
Width of band (MHz)	3	6.0	MHz total
Width of channel	0.025		
		120.0	FDD channels within band
Reuse group factor	21		(Mixture of portables and mobiles)
		5.7	Channels per cell
Guard channels	2		(At band edge)
Interoperability channels	20		(Reserve for direct mode operations)
		98.0	**Traffic channels**
Traffic/channel	4		Slots/channel
Data/channel	7.2		kbit/s/slot
Overhead and signalling	1.25		(36 kbit/s per channel total)
		168.0	**kbit/s/cell**
		3.0	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		56.0	**kbit/s/cell/MHz on outbound or inbound channel**
Speech improvement	1.05	58.8	kbit/s/cell/MHz on outbound or inbound channel with speech improvement
All improvements	1.1	61.6	kbit/s/cell/MHz on outbound or inbound channel with all improvements

Example 5: Wideband technologies for data and low rate video.

Technology capable of meeting requirement of United States of America 700 MHz public safety band for 384 kbit/s within 150 kHz channel bandwidth.

C4 and C5 Net system capability calculation

384 kbit/s / 150 kHz estimate			
Width of band (MHz)	4.8	9.6	MHz total
Width of channel	0.15		MHz
		32.0	FDD channels within band
Reuse group factor	12		
		2.7	Channels per cell
Guard channels	4		(At band edge)
I/O channels	12		
		16.0	**Traffic channels**
Traffic/channel	1		Slots per channel
Data/channel	192		kbit/s/slot
Overhead and signalling	2		(192 kbit/s per channel total)
		512.0	**kbit/s/cell**
		4.8	MHz bandwidth on outbound or inbound channel
		Total capacity available	
		106.7	kbit/s/cell/MHz on outbound or inbound channel
Speech improvement	1.05	**112.0**	**kbit/s/cell/MHz on outbound or inbound channel with speech improvement**
All improvements	1.1	117.3	kbit/s/cell/MHz on outbound or inbound channel with all improvements

Data: assume 3/4 coding or 144 kbit/s source data, 48 kbit/s FEC, 192 kbit/s overhead.

Video: assume 1/2 coding or for medium quality full motion video at 10 frames/s

~50 kbit/s for video and 4.8 kbit/s for voice channel, 55 kbit/s FEC, 110 kbit/s overhead

Attachment D of Appendix 1 to Annex 4

Example: Public safety and disaster relief population density data

England and Wales

Population = ~ 52.2 million England = ~ 49.23 million

Wales = ~ 2.95 million

Land Area = ~151 000 km^2 England = ~ 130 360 km^2

Wales = ~ 20 760 km^2

England population density = 346 pop/km^2 = 100 000 pop/289 km^2

London population = 7 285 000 people

London area = 1 620 km^2

London population density = 4 496 pop/ km^2 = 100 000 pop/ 22.24 km^2

Police officer strength[6]

	Total	Density /100 000
Police officers (ordinary duty)	123 841	237.2
Police officers (secondary assignments)	2 255	4.3
Police officers (outside assignments)	702	1.3
Total	126 798	242.9

Full time civilian staff[7]

Full time	48 759	93.4
Part time equivalent (7 897 staff)	4 272	8.2
Total	53 031	101.6

Average densities (ordinary officers)

Average = 237.2 officers per 100 000 population
Urban = 299.7
Non-urban = 201.2

8 largest metro = 352.4

Lowest rural = 176.4
Officer/civilian = 126 798/53 031 = 2.4 officers/civilian staff

Police officer distribution by rank

Chief Constable	49	0.04%
Assistant Chief Constable	151	0.12%
Superintendent	1 213	0.98%
Chief Inspector	1 604	1.30%
Inspector	5 936	4.80%
Sergeant	18 738	15.1%
Constable	96 150	77.6%

Other[8]

Special Constables	16 484
Traffic Wardens	3 342 full time equivalents (3 206 full-time and 242 part-time)

6 Source: Police Service Personnel, England and Wales, as of 31 March 1999, by Julian Prime and Rohith Sen-gupta @ Home Office, Research Development & Statistics Directorate.

7 Includes National Crime Squad (NCS) & National criminal Intelligence Service (NCIS) civilian staffing.

8 Not included in totals above.

Fire Brigade

Staffing in England and Wales (43 brigades)

Paid	35 417
Retained (part-time or volunteer)	14 600
	50 082

London: assume 126 798/35 417 = 3.58 police/fire

or about 98 fires/100 000 population in London

Fire radio inventory ~24 500 radios

50% penetration of radios into total

70% penetration of full-time fire fighters

London PPDR estimates

PPDR category	PPDR population	PPDR penetration rate for narrowband voice
Police	25 498	100%
Other Police Functions	6 010	10%
Police Civilian Support (dispatchers, technicians, etc.)	13 987	10%
Fire Brigade	7 081	70%
Part-time Fire	2 127	10%
Fire Civilian Support	–	0%
Emergency Medical	–	0%
EMS Civilian Support	–	0%
Services généraux du gouvernement	–	0%
General Government	–	0%
Other PPDR Users	–	0%

Attachment E
of Appendix 1 to Annex 4

Example calculation

	IMT-2000 methodology (Rec. UIT-R M.1390)		**London TETRA Narrowband voice service**		
A	Geographic considerations				
A1	Select operational environment type. Each environment type basically forms a column in calculation spreadsheet. Do not have to consider all environments, only the most significant contributors to spectrum requirements. Environments may geographically overlap. No user should occupy any two operational environments at one time	Environment = "e" Combination of user density and user mobility: Density: dense urban, urban, suburban, rural; Mobility: in-building, pedestrian, vehicular. Determine which of the possible density/mobility environments co-exist AND create greatest spectrum demand		**Urban pedestrian and mobile**	**Urban pedestrian and mobile**
A2	Select direction of calculation, uplink vs downlink or combined	Usually separate calculations for uplink and downlink due to asymmetry in some services		**Uplink**	**Downlink**
A3	Representative cell area and geometry for each operational environment type	Average/typical cell geometry (m): radius for omni-directional cells; radius of vertex for sectored hexagonal cells		**5**	
A4	Calculate representative cell area	Omni cells: circular = $\pi \cdot R^2$; hexagonal = $2.6 \cdot R^2$; Hex 3-sector = $2.6 \cdot R^2/3$ km^2		**65**	
B	Market and traffic considerations				
B1	Telecommunication services offered	Corresponding net user bit rate (kbit/s)		**7.2 kbit/s = 4.8 kbit/s vocoded voice = 2.4 kbit/s FEC**	

	IMT-2000 methodology (Rec. UIT-R M.1390)		London TETRA Narrowband voice service		
B2	Population density	Total population = sum (POP by category)		**54 703**	**Total PPDR population within area under consideration**
				Population (POP) by PPDR category	Penetration (PEN) rate within PPDR category
					(Narrowband voice)
			Police	25 498	1.00
			Other Police	6 010	0.10
			Police Civilian Support	13 987	0.10
			Fire	7 081	0.70
			Part-time Fire	2 127	0.10
			Fire Civilian Support	0	0.10
			EMS	0	0.50
			EMS Civilian Support	0	0.10
			General Government	0	0.10
			Other PPDR Users	0	0.10
		= SUM (POP × PEN)		**32 667,1**	**PPDR population using NB voice service**
		Area under consideration	308.9 square miles	**1 620**	**km^2**
	Number of persons per unit of area within the environment under consideration. Population density may vary with mobility	Potential user per km^2		**33.8**	**Total POP/km^2**

	IMT-2000 methodology (Rec. UIT-R M.1390)		London TETRA Narrowband voice service		
B3	Penetration rate Percentage of persons subscribing to a service within an environment. Person may subscribe to more than one service, therefore, total penetration rate of all services within environment can exceed 100%		= PEN into PPDR category × PPDR category POP/total PPDR POP	By category (Police = Police PEN × Police POP)	By Category (Police = Police PEN × Police POP)/Total PPDR POP
			Police	25 498.00	0.466
			Other Police	601.00	0.011
			Police Civilian Support	1 398.70	0.026
			Fire	4 956.70	0.091
			Part-time Fire	212.70	0.004
			Fire Civilian Support	0.00	0.000
			EMS	0.00	0.000
			EMS Civilian Support	0.00	0.000
			General Government	0.00	0.000
			Other PPDR Users	0.00	0.000
		= % of total PPDR POP	**Total PPDR penetration**	**59.717**	**% using NB voice**
B4	Users/cell Represents the number of people actually subscribing to the service "s" within a cell in environment "e"	Users/cell = POP density × PEN rate × Cell area Dependent upon population density, cell area, and service penetration rate in each environment		**1 311**	**PPDR NB voice users per cell**

	IMT-2000 methodology (Rec. UIT-R M.1390)		London TETRA Narrowband voice service		
B5	Traffic parameters			**Uplink**	**downlink**
	Busy hour call attempts (BCHA)	Calls/busy hour	From PSWAC	0.0073284 E/busy hour	0.0463105 E/busy hour
	Average number of calls/sessions attempted to/from average user during busy hour		**Per PPDR NB voice user**	**3.535**	**6.283**
	Effective call duration Average call/session duration during busy hours	Seconds/call	**Per PPDR NB voice user**	**7.88069024**	**26.53474455**
	Activity factor Percentage of time that resource is actually used during a conversation/session. Packet data may be bursty and resource is only used a small percentage of time that session is active. If voice is only transmitted when user speaks it does not tie up resource during pauses in speech or when listening	Dispatch voice – each conversation ties up both sides of duplex channel	**Per PPDR NB voice user**	**1**	**1**
B6	Traffic/user Average traffic in call-seconds generated by each user during busy hour	Call-seconds per user = Busy hour attempts × Call duration × Activity	**PPDR NB voice traffic/user**	**27.9**	**166.7**
B7	Offered traffic/cell Average traffic generated by all users within a cell during the busy hour (3 600 s)	Erlangs = Traffic/user × User/cell/3 600	**PPDR NB voice traffic cell**	**10.14**	**60.70**

	IMT-2000 methodology (Rec. UIT-R M.1390)		London TETRA Narrowband voice service		
B8	Establish quality of service (QOS) function parameters			**Uplink**	**Downlink**
	Group size Number of cells in a group. Because cellular system deployment and technologies provide some measure of traffic "sharing" between adjacent cells, traffic versus QoS is considered within a grouping of cells	12 (portable only) or 21 (portable + mobile) Typical cellular grouping is 1 cell surrounded by 6 adjacent cells for a group size of 7. Traffic/cell is multiplied by group size and quality of service (or blocking function) is applied to grouping. Answer is divided by group size to restore to valuation per cell		**21**	**21**
	Traffic per group	= Traffic/cell (E) × Group size	**PPDR NB voice traffic group**	**213.00**	**1 274.70**
	Service channels per group Determine number of channels required to support traffic from each service, round to next higher whole number	= apply grade of service formulas across group Circuit = Erlang B with 1% blocking. Used Erlang = 1.5, assuming that dispatch voice in broken into multiple systems with no more than 20 channels per site		**1.50**	**1.50**
			PPDR NB voice service channels per group	**319.50**	**1 912.05**
C	Technical and system considerations			**Uplink**	**Downlink**
C1	Service channels per cell needed to carry offered load Actual number of "channels" that must be provisioned within each cell to carry intended traffic	= Service channels per group/Group size	**PPDR NB voice service channels per cell**	**15.21**	**91.05**
C2	Service channel bit rate (kbit/s) Service channel bit rate equals net user bit rate, plus any additional increases in bit rate due to coding factors and/or overhead signalling	= Net user bit rate × Overhead factor × Coding factor This is where coding and overhead factors are included. For coding factor = 1, and overhead factor = 1, = B1 × 1 × 1 = Net user bit rate	9.6 kbit/s includes coding and overhead **PPDR NB voice service channel bit rate**	**9**	**9**

	IMT-2000 methodology (Rec. UIT-R M.1390)		**London TETRA Narrowband voice service**		
C3	Calculate traffic (Mbit/s) Total traffic to be transmitted within the area of study – includes all factors; user traffic (call duration, busy hour call attempts, activity factor, net channel bit rate) environment, service type, direction of transmission (up/down link), cell geometry, quality of service, traffic efficiency (calculated across a group of cells), and service channel bit rate (including coding and overhead factors)	= Service channels/Cell × Service channel bit rate	**PPDR NB voice traffic (Mbit/s)**	**0.137**	**0.819**
C4	Net system capability Measure of system capacity for a specific technology. Related to spectral efficiency. Requires complex calculation or simulation to determine net system capability for a specific technology deployed in a specific network configuration	Trade-offs between net system capability and QoS. May include the following factors; spectral efficiency of technology, E_b/N_0 requirements, C/I requirements, frequency re-use plan, coding/signalling factors of radio transmission technology, enviroment, deployment model			
C5	Calculate for GSM model	Calculation for TETRA TDMA using 25 kHz bandwidth channels, 21 cell re-use (mobile + portable), 4 traffic slots per carrier, ignoring signalling channels, 400 MHz bandplan, FDD with 2 × 3 MHz (120 RF channels - 20 DMO channels –2 guard channels at edge of band), data rate of 7.2 kbits/s on each traffic slot, a factor of 1.25 for overhead and coding. Net system capacity for TETRA TDMA = 56.0 kbit/s/MHz/cell	**TETRA**	**0.056**	**0.056**

	IMT-2000 methodology (Rec. UIT-R M.1390)		**London TETRA Narrowband voice service**		
D	Spectrum results			**Uplink**	**Downlink**
D1-D4	Calculate individual components	Freq = Traffic/Net system capability	**PPDR NB voice (MHz)**	**2.445**	**14.633**
D5	Weighting factor for each environment (alpha) Weighting of each environment relative to other environments - alpha may vary from 0 to 1, correct for non-simultaneous busy hours, correct for geographic offsets	= Freq × alpha If all environments have coincident busy hours and all three environments are co-located,, then alpha = 1	**Alpha = 1**	**1**	**1**
			PPDR NB voice (MHz)	**2.445**	**14.633**
D6	Adjustment factor (beta)	Freq(total) = beta × sum (alpha × Freq)			
	Adjustment of all environments to outside effects – multiple operators/users (decreased trunking or spectral efficiency), guardbands, sharing with other services within band, technology modularity, etc.	For dispatch voice model, assuming one system and fact that guardbands were included in C5, then beta = 1. Multiple systems, such as one for Police and one for Fire/EMS may decrease efficiency and beta would be > 1	**Beta = 1**	**1**	
D7	Calculate total spectrum		**PPDR NB voice TOTAL (MHz)**	**17.078 MHz**	

Attachment F
of Appendix 1 to Annex 4

Example narrowband and wideband calculation summaries

London narrowband voice, message, and image

Narrowband PPDR category	London users	Penetration rates NB voice	NB message	NB image
Police	25 498	1.00	0.5	0.25
Other Police	6 010	0.10	0.05	0.025
Police Civilian Support	13 987	0.10	0.05	0.025
Fire	7 081	0.70	0.35	0.175
Part-time Fire	2 127	0.10	0.05	0.025
Fire Civilian Support	0	0.10	0.05	0.025
EMS	0	0.50	0.25	0.125
EMS Civilian Support	0	0.10	0.05	0.025
General Government	0	0.10	0.05	0.025
Other PPDR Users	0	0.10	0.05	0.025
Total – PPDR Users	**54 703**	32 667	16 334	8 167
Spectrum by "service environment" (MHz)		17.1	1.4	4.2
Narrowband spectrum 22.7 MHz				

Other parameters:				
Environment	Urban pedestrian and mobile			
Cell radius (km)	5			
Study area (km^2)	1 620			
Cell area (km^2)	65	(calculated)		
Cells per study area	25	(calculated)		
Net user bit rate	9 kbit/s (7.2 kbit/s per slot + 1.8 kbit/s channel overhead)			
	= 4.8 kbit/s speech, data, or image per slot			
	+ 2.4 kbit/s FEC per slot			
	+ 1.8 kbit/s channel overhead and signalling			
		NB voice	NB data	NB image
		Uplink	Uplink	Uplink
Erlangs per busy hour	(From PSWAC)	0.0077384	0.0030201	0.0268314
Busy hour call attempts		3.54	5.18	3.00
Effective call duration		7.88	2.10	32.20
Activity factor		1	1	1
		Downlink	Downlink	Downlink
Erlangs per busy hour	(From PSWAC)	0.0463105	0.0057000	0.0266667
Busy hour call attempts		6.28	5.18	3.00
Effective call duration		26.53	3.96	32.00
Activity factor		1	1	1
Group size	21			
Grade of service factor	1.50			
Net system capacity	0.0560	kbit/s/MHz/cellule		
Alpha factor	1			
Beta factor	1			

New York City narrowband voice, message, and image

Narrowband PPDR category	New York users	Penetration rates NB voice	NB message	NB image
Police	39 286	0.70	0.35	0.175
Other Police	0	0.10	0.05	0.025
Police Civilian Support	8 408	0.10	0.05	0.025
Fire	11 653	0.70	0.35	0.175
Part-time Fire	0	0.10	0.05	0.025
Fire Civilian Support	4 404	0.10	0.05	0.025
EMS	0	0.50	0.25	0.125
EMS Civilian Support	0	0.10	0.05	0.025
General Government	21 217	0.10	0.05	0.025
Other PPDR Users	3 409	0.10	0.05	0.025
Total – PPDR Users	**88 377**	**39 401**	**19 701**	**9 850**
Spectrum by “service environment” (MHz)		51.8	4.2	20.0
Narrowband spectrum	**76.0 MHz**			

Other parameters:				
Environment	Urban pedestrian and mobile			
Cell radius (km)	4			
Study area (km2)	800			
Cell area (km2)	41.6	(calculated)		
Cells per study area	19	(calculated)		
Net user bit rate	9.6 kbit/s			
	= 4.8 kbit/s speech, data, or image			
	+ 2.4 kbit/s FEC			
	+ 2.4 kbit/s overhead and signalling			
		NB voice	NB data	NB image
		Uplink	Uplink	Uplink
Erlangs per busy hour	(From PSWAC)	0.0077384	0.0030201	0.0268314
Busy hour call attempts		3.54	5.18	3.00
Effective call duration		7.88	2.10	32.20
Activity factor		1	1	1
		Downlink	Downlink	Downlink
Erlangs per busy hour	(From PSWAC)	0.0463105	0.0057000	0.0266667
Busy hour call attempts		6.28	5.18	3.00
Effective call duration		26.53	3.96	32.00
Activity factor		1	1	1
Group size	21			
Grade of service factor	1.50			
Net system capacity	0.0308	kbit/s/MHz/cell		
Alpha factor	1			
Beta factor	1			

New York City wideband data and video

Narrowband PPDR category	New York users	Penetration rates WB data	WB video
Police	39 286	0.23	0.14
Other Police	0	0.01	0.01
Police Civilian Support	8 408	0.01	0.01
Fire	11 653	0.28	0.20
Part-time Fire	0	0.01	0.01
Fire Civilian Support	4 404	0.01	0.01
EMS	0	0.31	0.17
EMS Civilian Support	0	0.01	0.01
General Government	21 217	0.01	0.03
Other PPDR Users	3 409	0.01	0.01
Total – PPDR Users	**88 377**	12 673	8 629
Spectrum by “service environment” (MHz)		18.3	19.5
Narrowband spectrum 37.9 MHz			

Other parameters:				
Environment	Urban pedestrian and mobile			
Cell radius (km)	3.0			
Study area (km^2)	800			
Cell area (km^2)	23.4	(calculated)		
Cells per study area	34	(calculated)		
Net user bit rate	Wideband video		Wideband data	
	(10 frames/s)		384 kbit/s	
	220 kbit/s		=144 kbit/s data	
	= 55 kbit/s video and voice		+48 kbit/s FEC	
	+55 kbit/s FEC		+192 kbit/s overhead	
	+110 kbit/s overhead			
Erlangs per busy hour	Uplink		Uplink	Uplink
Busy hour call attempts	0.0250	(calculated)	0.0008	0.0083
Effective call duration	3		3	3
Activity factor	30 s		1	10
	1		1	1
Group size	12			
Grade of service factor	1.50			
Net system capacity	0.1067	kbit/s/MHz/cell		
Alpha factor	1			
Beta factor	1			

Appendix 2
to Annex 4

PPDR spectrum calculation based on generic city analysis
(demographic population)

1 Generic City Approach

Instead of looking at specific cities, the following analysis examines several medium sized cities in several countries. This analysis is based upon the average density of police officers relative to the general demographic population and the ratio of police to other public protection providers. From this analysis, a generic example of the relationship between the different PPDR user categories and demographic population density has been developed. This approach shows the optimum PPDR spectrum requirement based on the size of demographic population, that is, the amount of PPDR spectrum requirement based on the idealistic amount of PPDR users in a city based on demographic population size.

The police and PPDR densities were examined from national statistics and city budgets for the United States, Canada, Australia, and England. Statistics for police show a national average density in the 180 police per 100 000 population to 250 police per 100 000 population. The density in urban areas varies from about 25% above the national average for medium density cities to >100% above the national average for dense urban cities. The density in suburban areas varies from about 25% above the national average for suburbs of medium density cities to 50% above the national average for suburbs of dense urban cities.

Fire and EMS/Rescue levels were harder to determine because they are often combined together. Information was used for cities where they were separate, and ratios of the various PP and DR categories were determined relative to the police population density. For example, ratios for fire fighters were in the range of 3.5 to 4 police officers per fire fighter (25 to 30%). Where Rescue/Emergency Medical/Ambulance could be separated out, ratios for Rescue/EMS were in the range of 3.5 to 4 fire fighters per Rescue/EMS (25 to 30%).

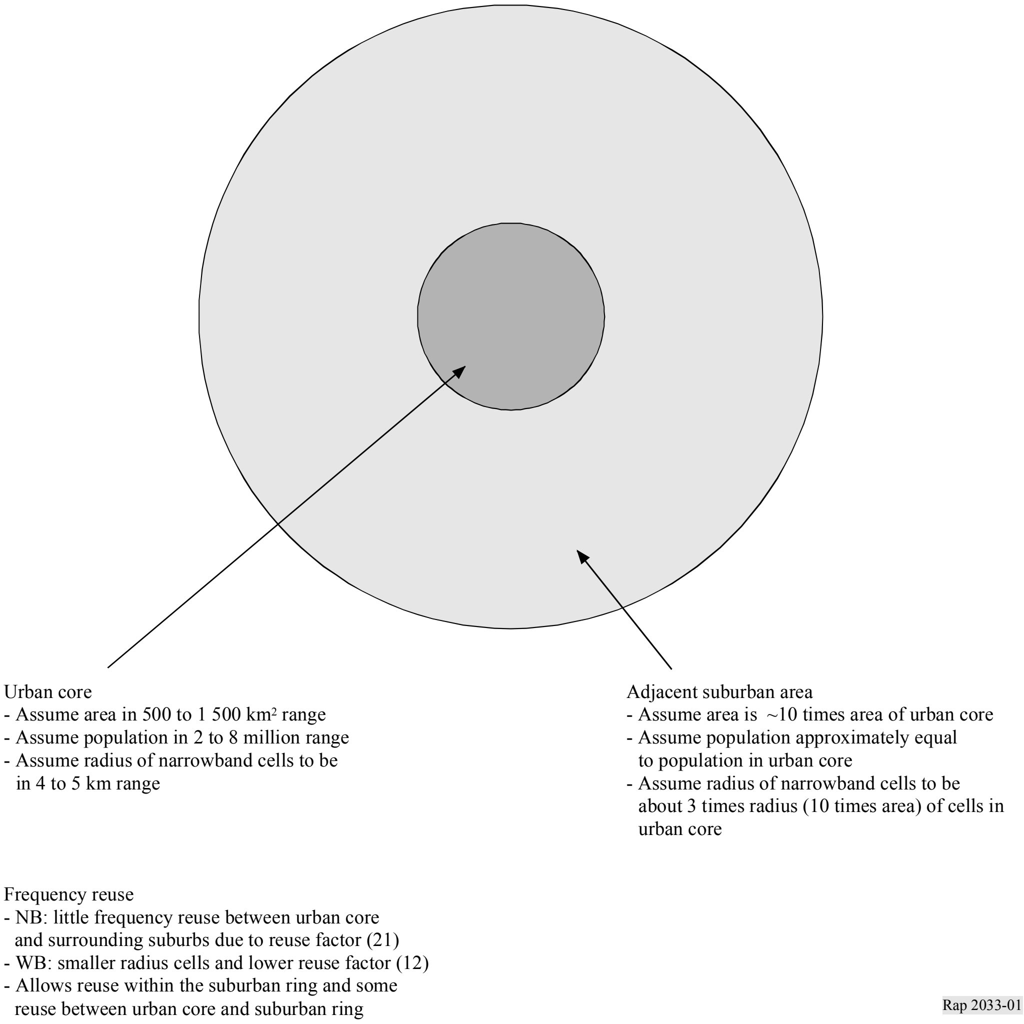
In the generic examples below, and for simplicity, only two densities are used, 180 and 250 police per 100 000 population. Also for simplicity, only two types of cities were analysed: a medium size city (2.5 million population) and a large city (8 million population). This probably underestimates the PPDR density in large urban areas where there are many examples of police densities in the range of 400-500 police per 100 000 population.

The "doughnut" effect was also examined, where frequencies used in the urban center can not be reused in the suburbs immediately adjacent to the urban area. In ITU-R contributions from the 2000-2003 study period, many of the cities included both the urban and suburban areas together in a single spectrum requirement calculation. Cell size had to be averaged and PPDR user density was lowered. In retrospect, each area should have been treated separately, and the spectrum requirements added together.

Numerous urban areas were examined. Most had a central urban core with a dense population. There was also a suburban ring around the urban core that contained about the same amount of population, but was about 5 to 20 times the area of the urban core. The examples below use a ratio of 10:1 for suburban to urban area. Assuming 4 to 5 km radius cell sizes for the urban core, typical cell sizes in the suburbs should be about 10 times larger in area or ~3 times larger in radius.

FIGURE 1

Metropolitan Area
(Urban core and adjacent suburbs)



2 PPDR categories

Three classes of users were defined, which is basically re-grouping the PPDR categories by penetration rates:

Primary users (usage with 30% penetration rate) = PP users normally operating within the geographic area on a day-to-day basis = local police, fire fighters, and emergency medical/rescue.

Secondary users (usage with 10% penetration rate) = other police (state, district, province, federal, national, special operations, investigators), part-time or volunteer police/fire, general government workers, civil protection agencies, military/army, utility workers, disaster relief workers.

Support users (usage with <10% penetration rate) = civilian support.

Penetration rate and PPDR category data used to calculate spectrum requirements

Narrowband and wideband CATEGORY name and number of USER's		Services summary	NB voice	NB message	NB status	WB data	WB video
User category	**Users**		**Penetration rate summary**				
Primary – Local Police	5 625		0.300	0.300	0.300	0.250	0.125
Secondary – Law Enforcement/ Investigators	563		0.100	0.100	0.100	0.010	0.010
Secondary – Police Functions	0		0.100	0.100	0.100	0.010	0.010
Police Civilian Support	1 125		0.100	0.000	0.000	0.010	0.010
Primary – Fire Fighters	1 631		0.300	0.300	0.300	0.250	0.125
Fire Civilian Support	326		0.100	0.000	0.000	0.010	0.010
Primary – Rescue/Emergency Medical	489		0.300	0.300	0.300	0.250	0.125
Rescue/EMS Civilian Support	98		0.100	0.000	0.000	0.010	0.010
Secondary – General Government and Civil Agencies	563		0.100	0.100	0.100	0.010	0.010
Secondary – Volunteers and other PPDR Users	281		0.100	0.100	0.100	0.010	0.010
Total Users	10 701						

Primary users are the users that local public protection system would be designed to handle. A local system would be designed to handle "average busy hour" traffic plus a loading factor to be able to handle peak loads with a reasonable grade of service.

Part of the assumption is that many secondary users may have their own communications system and loading added to local public protection system is for coordination between the secondary users and the primary users.

Disaster scenario

Disaster occurs and personnel from surrounding areas, national government, and international agencies come to support the local agencies. There is immediate need for emergency workers to handle fires and to rescue injured people. Later arrivals are investigators and personnel to clean up the damage.

For disaster response – the following assumptions were made:

– *Civilian support* (<10% penetration rate): No increase in the number of civilian support workers for police/fire/EMS/rescue. The usage remains within the original system design parameters (30% penetration rate, 1.5 GoS peaking factor).

– *Police*: No increase in the number of local police. The usage remains within the original system design parameters (30% penetration rate, 1.5 GoS peaking factor).

– *Other Police*: Increase in personnel providing police functions equal to 30% of local police population, but at a lower secondary level (10% penetration rate). These are personnel who come from outside the area to supplement local police.

– *Investigators and Law Enforcement*: The population doubles as additional investigators move into the disaster area.

– *Fire and EMS/Rescue*: A 30% increase in the number of users. Users from surrounding areas immediately move into the disaster area and operate on the local system or set up additional communication systems. The need for communications is very great. Operate at primary level (30% penetration rate).

– *Secondary level users* (10% penetration rate): Double the number of general government users, volunteers, civil agency users, utility users, etc., who need to communicate with primary users or need to use the local network for communications.

Where is the disaster?

Look at three disaster scenarios:

1 No disaster = normal day-to-day operations

2 Disaster only in urban area

3 Disaster only in suburban area

3 Spectrum requirements

Calculate spectrum requirements for:

– Urban day-to-day

– Urban disaster

– Suburban day-to-day

– Suburban disaster

– Spectrum requirements for the three disaster scenarios:

(Instead of worst case analysis)

Urban and suburban systems designed to handle "average busy hour" traffic loading plus a 1.5 GoS factor to handle emergency loading by the normal PPDR users. Disaster operations assumes that additional, outside PPDR personnel are added to the system.

a) *Normal day-to-day operations*:

The amount of spectrum required for NB equals the sum of the urban and suburban spectrum calculations. The assumption is that spectrum used in the urban area can not be reused in the adjacent suburban area, due to large cell size and large reuse factor.

The amount of spectrum required for WB equals the sum of the urban and half of the suburban spectrum calculation. The assumption is that spectrum used in the urban area can be reused in the adjacent suburban area, due to the smaller cell size and smaller reuse factor. Also, because the urban area sits in middle of the suburban area, there is some additional separation, which would allow additional frequency reuse between suburban sites.

b) *Urban disaster operations*:

The amount of spectrum required for NB equals the sum of the urban disaster and the suburban non-disaster spectrum calculation.

The amount of spectrum required for WB equals the sum of the urban disaster and half of the suburban non-disaster spectrum calculation.

c) *Suburban disaster operations*:

The amount of spectrum required for NB equals the sum of the urban non-disaster and the suburban disaster spectrum calculation.

The amount of spectrum required for WB equals the sum of the urban non-disaster and half of the suburban disaster spectrum calculation.

Medium metropolitan area

Calculated spectrum requirements using a PPDR calculator spreadsheet.

Medium metropolitan area (Urban population ≅ 2.5 million and area ≅ 600 km²) (Suburban population ≅ 2.5 million and area ≅ 6 000 km²)					
Medium PPDR density (180 Police per 100 000 population)			**High PPDR density** (250 police per 100 000 population)		
Urban			**Urban**		
NB day-to-day	15.5	MHz	NB day-to-day	21.5	MHz
WB day-to-day	16.2	MHz	WB day-to-day	22.6	MHz
Disaster NB	18.4	MHz	Disaster NB	25.6	MHz
Disaster WB	17.8	MHz	Disaster WB	24.7	MHz
Suburban			**Suburban**		
NB day-to-day	12.9	MHz	NB day-to-day	17.9	MHz
WB day-to-day	13.5	MHz	WB day-to-day	18.8	MHz
Disaster NB	15.4	MHz	Disaster NB	21.4	MHz
Disaster WB	14.8	MHz	Disaster WB	20.6	MHz
Normal day-to-day			**Normal day-to-day**		
NB (urban + suburban)	28.40	MHz	NB	39.40	MHz
WB (urban + 1/2 suburban)	22.95	MHz	WB	32.00	MHz
	51.35	MHz		71.40	MHz
Suburban disaster			**Suburban disaster**		
NB	30.90	MHz	NB	42.90	MHz
WB	23.60	MHz	WB	32.90	MHz
	54.50	MHz		75.80	MHz
Urban disaster			**Urban disaster**		
NB	31.30	MHz	NB	43.50	MHz
WB	24.55	MHz	WB	34.10	MHz
	55.85	MHz		77.60	MHz

The left-hand column shows the spectrum calculated for a medium PPDR user density and the right-hand column shows the spectrum calculated for a higher PPDR user density.

The top-half of the chart shows individual NB and WB spectrum calculations for normal "day-to-day" operations and for a disaster within the local area.

The total spectrum requirement is the sum of the urban and suburban calculations. For narrowband the assumption is that frequencies are not reused between the two areas, so the total is the sum of the NB urban and the NB suburban requirements. For wideband, the assumption is that some frequencies can be reused, therefore, the total is the sum of the wideband urban requirement and half of the wideband suburban requirement.

The bottom half of the chart shows the spectrum calculated for a disaster in either the urban area or the suburban area, where there is a significant increase in the number of users (up to 30% for primary users).

Normal day-to-day operations for this generic medium size city require from 51 MHz to 71 MHz depending on whether it is located in a country with a medium PPDR density or a high PPDR density.

If a disaster scenario described above occurs in the suburban area, then the NB/WB spectrum requirement increases by about 6%. If a disaster occurs in the urban area, then NB/WB spectrum requirement increases by about 9%.

Disaster operations for this generic medium size city require from 55 MHz to 78 MHz depending on where the disaster occurs and whether it is located in a country with a medium PPDR density or a high PPDR density.

The broadband spectrum requirement needs to be added. Since broadband will cover very small radius "hot spots", the broadband frequencies can be reused throughout the urban and suburban area. ITU-R contributions from the 2000-2003 study period have shown broadband spectrum requirements to be in the 50-75 MHz range.

Therefore, for a generic medium size city, the total spectrum requirement is in the range of 105 to 153 MHz to handle the type of disaster scenario described above.

The following two tables show the breakout of PPDR users and narrowband and wideband services in a medium-sized metropolitan area.

Medium metropolitan area calculated for 180 police officers per 100 000 population

Spectrum Requirements – Generic City Calculator		Re-Formatted		July 2002
Metropolitan Study Area	Medium Metropolitan Area			Input Data
Population of Urban Area	2 500 000	People	**1.0**	Ratio Suburban/Urban Population
Population of Surrounding Suburban Area	2 500 000	People		Ratio should be near 1.0 (Range of 0.5 × to 1.5 × of Urban Population)
Area of Urban Center	600	km^2	**10.0**	Ratio Suburban/Urban Area
Area of Surrounding Suburbs	6 000	km^2		Ratio should be near 10.0 (Range of 5 × to 15 × of Urban Area)
Urban Population Density	4 167	People/km^2		
Suburban Population Density	417	People/km^2		
"Large" or "Medium" City	MED	If Urban Population Density > 5 000 people/km^2, then this is a large city, OR if Urban population > 3 000 000 people, then this is a large city, otherwise this is a medium city		
Police User Density (national average)	180.0	Police per 100 000 population		

CATEGORY name and number of USERS User Category	Urban Day-to-Day	Urban Disaster	Suburban Day-to-Day	Suburban Disaster
	Population	Population	Population	Population
Primary – Local Police	6 750	6 750	5 625	5 625
Secondary – Law Enforcement/Investigators	675	1 350	563	1 125
Secondary – Police Functions	0	2 025	0	1 688
Police Civilian Support	1 350	1 350	1 125	1 125
Primary – Fire Fighters	1 958	2 545	1 631	2 121
Fire Civilian Support	392	392	326	326
Primary – Rescue/ Emergency Medical	587	763	489	636
Rescue/EMS Civilian Support	117	117	98	98
Secondary – General Government and Civil Agencies	675	1 350	563	1 125
Secondary – Volunteers and Other PPDR Users	338	675	281	563
Total	12 841	17 317	10 701	14 431

Medium metropolitan area calculated for 180 police officers per 100 000 population (*end*)

Narrowband	Urban Day-to-Day		Urban Disaster		Suburban Day-to-Day		Suburban Disaster	
	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)
NB Voice Service	3 143	13.8	3 743	16.4	2 619	11.5	3 119	13.7
NB Message Service	2 957	1.6	3 557	1.9	2 464	1.3	2 965	1.6
NB Status Service	2 957	0.1	3 557	0.1	2 464	0.1	2 965	0.1
Total Narrowband Spectrum Required (MHz)		**15.5**		**18.4**		**12.9**		**15.4**
Normal NB Day-to-Day	28.4 MHz	15.5	<	<	<	12.9		
NB Urban Disaster Scenario	31.3 MHz	<	<	18.4	<	12.9		
NB Suburban Disaster Scenario	30.9 MHz	15.5	<	<	<	<	<	15.4
Larger of the two NB Disaster Scenarios	31.3 MHz							
Wideband	Urban Day-to-Day		Urban Disaster		Suburban Day-to-Day		Suburban Disaster	
	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)
WB Data Service	2 359	15.7	2 587	17.2	1 966	13.1	2 156	14.3
WB Video Service	1 197	0.5	1 330	0.6	998	0.4	1 108	0.5
Total Wideband Spectrum Required (MHz)		**16.2**		**17.8**		**13.5**		**14.8**
						× 1/2		**× 1/2**
Normal WB Day-to-Day	23.0 MHz	16.2	<	<	<	6.8		
Urban WB Disaster Scenario	24.6 MHz	<	<	17.8	<	6.8		
Suburban WB Disaster Scenario	23.6 MHz	16.2	<	<	<	<	<	7.4
Larger of the two NB Disaster Scenarios	24.6 MHz							
Spectrum Requirement Totals	NB		WB		Sum			
Normal Day-to-Day	28.4	+	23.0	=	51.4	MHz		
Suburban Disaster Scenario	30.9	+	23.6	=	54.5	MHz		
Urban Disaster Scenario	31.3	+	24.6	=	55.9	MHz		

Medium metropolitan area calculated for 250 police officers per 100 000 population

Spectrum Requirements – Generic City Calculator				Re-Formatted	July 2002
Metropolitan Study Area	Medium Metropolitan Area				Input Data
Population of Urban Area	2 500 000	People	**1.0**	Ratio Suburban/Urban Population	
Population of Surrounding Suburban Area	2 500 000	People		Ratio should be near 1.0 (Range of 0.5 × to 1.5 × of Urban Population)	
Area of Urban Center	600	km^2	**10.0**	Ratio Suburban/Urban Area	
Area of Surrounding Suburbs	6 000	km^2		Ratio should be near 10.0 (Range of 5 × to 15 × of Urban Area)	
Urban Population Density	4 167	People/km^2			
Suburban Population Density	417	People/km^2			
"Large" or "Medium" City	MED	If Urban Population Density > 5 000 people/km^2, then this is a large city, OR if Urban population > 3 000 000 people, then this is a large city, otherwise this is a medium city			
Police User Density (national average)	250.0	Police per 100 000 population			

CATEGORY name and number of USERS User Category	Urban Day-to-Day	Urban Disaster	Suburban Day-to-Day	Suburban Disaster
	Population	Population	Population	Population
Primary – Local Police	9 375	9 375	7 813	7 813
Secondary – Law Enforcement/Investigators	938	1 875	781	1 563
Secondary – Police Functions	0	2 813	0	2 344
Police Civilian Support	1 875	1 875	1 563	1 563
Primary – Fire Fighters	2 719	3 534	2 266	2 945
Fire Civilian Support	544	544	453	453
Primary – Rescue/ Emergency Medical	816	1 060	680	884
Rescue/EMS Civilian Support	163	163	136	136
Secondary – General Government and Civil Agencies	938	1 875	781	1 563
Secondary – Volunteers and Other PPDR Users	469	938	391	781
Total	17 835	24 052	14 863	20 043

Medium metropolitan area calculated for 250 police officers per 100 000 population (*end*)

Narrowband	Urban Day-to-Day		Urban Disaster		Suburban Day-to-Day		Suburban Disaster	
	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)
NB Voice Service	4 365	19.2	5 199	22.8	3 638	16.0	4 333	19.1
NB Message Service	4 107	2.2	4 941	2.7	3 423	1.9	4 117	2.2
NB Status Service	4 107	0.1	4 941	0.1	3 423	0.1	4 117	0.1
Total Narrowband Spectrum Required (MHz)		**21.5**		**25.6**		**17.9**		**21.4**

Normal NB Day-to-Day	39.4 MHz	21.5	<	<	<	17.9		
NB Urban Disaster Scenario	43.5 MHz	<	<	25.6	<	17.9		
NB Suburban Disaster Scenario	42.8 MHz	21.5	<	<	<	<	<	21.4
Larger of the two NB Disaster Scenarios	43.5 MHz							

Wideband	Urban Day-to-Day		Urban Disaster		Suburban Day-to-Day		Suburban Disaster	
	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)
WB Data Service	3 277	21.8	3 593	23.9	2 731	18.2	2 994	19.9
WB Video Service	1 663	0.7	1 847	0.8	1 386	0.6	1 539	0.7
Total Wideband Spectrum Required (MHz)		**22.5**		**24.7**		**18.8**		**20.6**
						× 1/2		**× 1/2**

Normal WB Day-to-Day	31.9 MHz	22.5	<	<	<	9.4		
Urban WB Disaster Scenario	34.1 MHz	<	<	24.7	<	9.4		
Suburban WB Disaster Scenario	32.8 MHz	22.5	<	<	<	<	<	10.3
Larger of the two NB Disaster Scenarios	34.1 MHz							

Spectrum Requirement Totals	NB		WB		Sum	
Normal Day-to-Day	39.4	+	31.9	=	71.3	MHz
Suburban Disaster Scenario	42.8	+	32.8	=	75.7	MHz
Urban Disaster Scenario	43.5	+	34.1	=	77.6	MHz

Large metropolitan area

Calculated spectrum requirements using a PPDR calculator spreadsheet.

Large metropolitan area (Urban population ≅ 8.0 million and area ≅ 800 km²) (Suburban population ≅ 8.0 million and area ≅ 8 000 km²)					
Medium PPDR density (180 Police per 100 000 population)			**High PPDR density** (250 police per 100 000 population)		
Urban			**Urban**		
NB day-to-day	23.7	MHz	NB day-to-day	33.0	MHz
WB day-to-day	24.9	MHz	WB day-to-day	34.6	MHz
Disaster NB	28.3	MHz	Disaster NB	39.3	MHz
Disaster WB	27.4	MHz	Disaster WB	38.0	MHz
Suburban			**Suburban**		
NB day-to-day	19.8	MHz	NB day-to-day	27.4	MHz
WB day-to-day	20.7	MHz	WB day-to-day	28.7	MHz
Disaster NB	23.6	MHz	Disaster NB	32.7	MHz
Disaster WB	22.7	MHz	Disaster WB	31.5	MHz
Normal day-to-day			**Normal day-to-day**		
NB (urban + suburban)	43.50	MHz	NB	60.40	MHz
WB (urban + 1/2 suburban)	35.25	MHz	WB	48.95	MHz
	78.75	MHz		109.35	MHz
Suburban disaster			**Suburban disaster**		
NB	47.30	MHz	NB	65.70	MHz
WB	36.25	MHz	WB	50.35	MHz
	83.55	MHz		116.05	MHz
Urban disaster			**Urban disaster**		
NB	48.10	MHz	NB	66.70	MHz
WB	37.75	MHz	WB	52.35	MHz
	85.85	MHz		119.05	MHz

The left-hand column shows the spectrum calculated for a medium PPDR user density and the right-hand column shows the spectrum calculated for higher PPDR user density.

The top-half of the chart shows individual NB and WB spectrum calculations for normal “day-to-day” operations and for a disaster within the local area.

The total spectrum requirement is the sum of the urban and suburban calculations. For narrowband the assumption is that frequencies are not reused between the two areas, so the total is the sum of the NB urban and the NB suburban requirements. For wideband, the assumption is that some frequencies can be reused, therefore, the total is the sum of the wideband urban requirement and half of the wideband suburban requirement.

The bottom half of the chart shows the spectrum calculated for a disaster in either the urban area or the suburban area, where there is a significant increase in the number of users (up to 30% for primary users).

Normal day-to-day operations for this generic large city requires from 79 MHz to 109 MHz depending on whether it is located in a country with a medium PPDR density or a high PPDR density.

If a disaster scenario described above occurs in the suburban area, then the NB/WB spectrum requirement increases by about 6%. If disaster occurs in the urban area, then the NB/WB spectrum requirement increases by about 9%.

Disaster operations for this generic large city require from 84 MHz to 119 MHz depending on where the disaster occurs and whether it is located in a country with a medium PPDR density or a high PPDR density.

The broadband spectrum requirement needs to be added. Since broadband will cover very small radius “hot spots”, the broadband frequencies can be reused throughout the urban and suburban area. ITU-R contributions from the 2000-2003 study period have shown broadband spectrum requirements to be in the 50-75 MHz range.

Therefore, for a generic large city, the total spectrum requirement is in the range of 134 to 194 MHz to handle the type of disaster scenario described above.

The following two tables show the breakout of PPDR users and narrowband and wideband service in a large-sized metropolitan area.

Large metropolitan area calculated for 180 police officers per 100 000 population

Spectrum Requirements – Generic City Calculator		Re-Formatted		July 2002
Metropolitan Study Area	Medium Metropolitan Area			Input Data
Population of Urban Area	8 000 000	People	**1.0**	Ratio Suburban/Urban Population
Population of Surrounding Suburban Area	8 000 000	People		Ratio should be near 1.0 (Range of 0.5 × to 1.5 × of Urban Population)
Area of Urban Center	800	km²	**10.0**	Ratio Suburban/Urban Area
Area of Surrounding Suburbs	8 000	km²		Ratio should be near 10.0 (Range of 5 × to 15 × of Urban Area)
Urban Population Density	10 000	People/km²		
Suburban Population Density	1 000	People/km²		
“Large” or “Medium” City	LAR	If Urban Population Density > 5 000 people/km², then this is a large city, OR if Urban population > 3 000 000 people, then this is a large city, otherwise this is a medium city		
Police User Density (national average)	180.0	Police per 100 000 population		

CATEGORY name and number of USERS User Category	Urban Day-to-Day	Urban Disaster	Suburban Day-to-Day	Suburban Disaster
	Population	Population	Population	Population
Primary – Local Police	21 600	21 600	18 000	18 000
Secondary – Law Enforcement/Investigators	2 160	4 320	1 800	3 600
Secondary – Police Functions	0	6 480	0	5 400
Police Civilian Support	4 320	4 320	3 600	3 600
Primary – Fire Fighters	6 264	8 143	5 220	6 786
Fire Civilian Support	1 253	1 253	1 044	1 044
Primary – Rescue/ Emergency Medical	1 879	2 443	1 566	2 036
Rescue/EMS Civilian Support	376	376	313	313
Secondary – General Government and Civil Agencies	2 160	4 320	1 800	3 600
Secondary – Volunteers and Other PPDR Users	1 080	2 160	900	1 800
Total	41 092	55 415	34 243	46 179

Large metropolitan area calculated for 180 police officers per 100 000 population (*end*)

Narrowband	Urban Day-to-Day		Urban Disaster		Suburban Day-to-Day		Suburban Disaster	
	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)
NB Voice Service	10 058	21.2	11 979	25.2	8 382	17.6	9 982	21.0
NB Message Service	9 463	2.5	11 384	3.0	7 886	2.0	9 487	2.5
NB Status Service	9 463	0.1	11 384	0.1	7 886	0.1	9 487	0.1
Total Narrowband Spectrum Required (MHz)		**23.7**		**28.3**		**19.8**		**23.6**
Normal NB Day-to-Day	43.5 MHz	23.7	<	<	<	19.8		
NB Urban Disaster Scenario	48.1 MHz	<	<	28.3	<	19.8		
NB Suburban Disaster Scenario	47.3 MHz	23.7	<	<	<	<	<	23.6
Larger of the two NB Disaster Scenarios	48.1 MHz							

Wideband	Urban Day-to-Day		Urban Disaster		Suburban Day-to-Day		Suburban Disaster	
	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)
WB Data Service	7 549	24.1	8 279	26.4	6 291	20.0	6 899	22.0
WB Video Service	3 831	0.8	4 256	0.9	3 193	0.7	3 546	0.8
Total Wideband Spectrum Required (MHz)		**24.9**		**27.4**		**20.7**		**22.7**
						× 1/2		**× 1/2**
Normal WB Day-to-Day	35.3 MHz	24.9	<	<	<	10.3		
Urban WB Disaster Scenario	37.7 MHz	<	<	27.4	<	10.3		
Suburban WB Disaster Scenario	36.3 MHz	24.9	<	<	<	<	<	11.4
Larger of the two NB Disaster Scenarios	37.7 MHz							

Spectrum Requirement Totals	NB		WB		Sum	
Normal Day-to-Day	43.5	+	35.3	=	78.8	MHz
Suburban Disaster Scenario	47.3	+	36.3	=	83.6	MHz
Urban Disaster Scenario	48.1	+	37.7	=	85.8	MHz

Large metropolitan area calculated for 250 police officers per 100 000 population

Spectrum Requirements – Generic City Calculator			Re-Formatted	July 2002
Metropolitan Study Area	Medium Metropolitan Area			Input Data
Population of Urban Area	8 000 000	People	**1.0**	Ratio Suburban/Urban Population
Population of Surrounding Suburban Area	2 000 000	People		Ratio should be near 1.0 (Range of 0.5 × to 1.5 × of Urban Population)
Area of Urban Center	800	km^2	**10.0**	Ratio Suburban/Urban Area
Area of Surrounding Suburbs	8 000	km^2		Ratio should be near 10.0 (Range of 5 × to 15 × of Urban Area)
Urban Population Density	10 000	People/km^2		
Suburban Population Density	1 000	People/km^2		
"Large" or "Medium" City	LAR	If Urban Population Density > 5 000 people/km^2, then this is a large city, OR if Urban population > 3 000 000 people, then this is a large city, otherwise this is a medium city		
Police User Density (national average)	250.0	Police per 100 000 population		

CATEGORY name and number of USERS User Category	Urban Day-to-Day	Urban Disaster	Suburban Day-to-Day	Suburban Disaster
	Population	Population	Population	Population
Primary – Local Police	30 000	30 000	25 000	25 000
Secondary – Law Enforcement/Investigators	3 000	6 000	2 500	5 000
Secondary – Police Functions	0	9 000	0	7 500
Police Civilian Support	6 000	6 000	5 000	5 000
Primary – Fire Fighters	8 700	11 310	7 250	9 425
Fire Civilian Support	1 740	1 740	1 450	1 450
Primary – Rescue/ Emergency Medical	2 610	3 393	2 175	2 828
Rescue/EMS Civilian Support	522	522	435	435
Secondary – General Government and Civil Agencies	3 000	6 000	2 500	5 000
Secondary – Volunteers and Other PPDR Users	1 500	3 000	1 250	2 500
Total	57 072	76 965	47 560	64 138

Large metropolitan area calculated for 250 police officers per 100 000 population (*end*)

Narrowband	Urban Day-to-Day		Urban Disaster		Suburban Day-to-Day		Suburban Disaster	
	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)
NB Voice Service	13 969	29.4	16 637	35.1	11 641	24.5	13 864	29.2
NB Message Service	13 143	3.4	15 811	4.1	10 953	2.8	13 176	3.4
NB Status Service	13 143	0.1	15 811	0.2	10 953	0.1	13 176	0.1
Total Narrowband Spectrum Required (MHz)		**33.0**		**39.3**		**27.4**		**32.7**
Normal NB Day-to-Day	60.4 MHz	33.0	<	<	<	27.4		
NB Urban Disaster Scenario	66.8 MHz	<	<	39.3	<	27.4		
NB Suburban Disaster Scenario	65.7 MHz	33.0	<	<	<	<	<	32.7
Larger of the two NB Disaster Scenarios	66.8 MHz							
Wideband	Urban Day-to-Day		Urban Disaster		Suburban Day-to-Day		Suburban Disaster	
	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)	Busy Hour Users	Spectrum Required (MHz)
WB Data Service	10 485	33.5	11 498	36.7	8 738	27.8	9 582	30.5
WB Video Service	5 321	1.1	5 910	1.3	4 434	0.9	4 925	1.0
Total Wideband Spectrum Required (MHz)		**34.6**		**38.0**		**28.7**		**31.5**
						× 1/2		**× 1/2**
Normal WB Day-to-Day	49.0 MHz	34.6	<	<	<	14.4		
Urban WB Disaster Scenario	52.4 MHz	<	<	38.0	<	14.4		
Suburban WB Disaster Scenario	50.4 MHz	34.6	<	<	<	<	<	15.8
Larger of the two NB Disaster Scenarios	52.4 MHz							
Spectrum Requirement Totals	NB		WB		Sum			
Normal Day-to-Day	60.4	+	49.0	=	109.4	MHz		
Suburban Disaster Scenario	65.7	+	50.4	=	116.1	MHz		
Urban Disaster Scenario	66.8	+	52.4	=	119.1	MHz		

PPDR population density analysis

- National average for police officers in the range 180 or 250 police/100 000 population.
- Suburban PPDR populations based upon police density of 1.25 times the national average.
- Urban PPDR populations based upon police density of 1.5 times the national average.
- Day-to-day PPDR population estimates:
  - Local police – population based on national average
  - Law enforcement/investigators – 10% of police density
  - Secondary police (coming from outside) – none
  - Police civilian support – 20% of police density
  - Fire fighters – 29% of police density (~3.5 police per fire)
  - Fire civilian support – 20% of fire fighter density
  - Rescue/EMS – 30% of fire fighter density (~11.7 police per EMS)
  - EMS civilian support – 20% of rescue/EMS density
  - General Government – 10% of police density
  - Other PPDR users and volunteers – 5% of police density
- Changes in PPDR populations during a disaster:
  - Local police – population remains the same
  - Law enforcement/investigators – population doubles
  - Secondary police (coming from outside)
  - Additional population about 30% of local police
  - Police civilian support – population remains the same
  - Fire fighters (coming from outside) – 30% increase in fire population
  - Fire civilian support – population remains the same
  - Rescue/EMS (coming from outside) – 30% increase in fire population
  - EMS civilian support – population remains the same
  - General government – population doubles
  - Other PPDR users and volunteers – population doubles

Summary of formulas used to calculate population density

PPDR user category	PPDR density	Suburban normal	Changes for disaster	Suburban disaster
Primary – Local Police	For suburban areas use 1.25 times national average police density	D(sub) = Police density × 1.25 × population/ 100 000	Remains the same	D(sub)
Secondary – Law Enforcement/Investigators	10% of police density	0.10 × D(sub)	Doubles	2.0 × (0.10 × D(sub))
Secondary – Police Functions	0	0.0 × D(sub)	30% of police density	0.3 × D(sub)
Police Civilian Support	20% of police density	0.2 × D(sub)	Remains the same	0.2 × D(sub)
Primary – Fire Fighters	29% of police density	0.29 × D(sub)	29% increase	1.3 × 0.29 × D(sub)
Fire Civilian Support	20% of fire density	0.2 × (0.29 × D(sub))	Remains the same	0.2 × 0.29 × D(sub)
Primary – Rescue/ Emergency Medical	30% of fire density	0.3 × (0.29 × D(sub))	30% increase	1.3 × 0.29 × 0.5 × D(sub)
Rescue/EMS Civilian Support	20% of EMS density	0.2 × (0.3 × (0.29 × D(sub)	Remains the same	0.2 × 0.3 × 0.29 × D(sub)
Secondary – General Government and Civil Agencies	10% of police density	0.10 × D(sub)	Doubles	2.0 × 0.10 × D(sub)
Secondary – Volunteers and Other PPDR	5% of police density	0.05 × D(sub)	Doubles	2.0 × 0.05 × D(sub)
Primary – Local Police	For urban areas use 1.5 times national average police density	D(urb) = Police density × 1.50 × population/ 100 000	Remains the same	D(urb)
Secondary – Law Enforcement/Investigators	10% of police density	0.10 D(urb)	Doubles	2.0 × (0.10 × D(urb))
Secondary – Police Functions	0	0.0 × D(urb)	30% of police density	0.3 × D(urb)
Police Civilian Support	20% of police density	0.2 × D(urb)	Remains the same	0.2 × D(urb)
Primary – Fire Fighters	29% of police density	0.29 × D(urb)	29% increase	1.3 × 0.29 × D(urb)
Fire Civilian Support	20% of fire density	0.2 × (0.29 × D(urb))	Remains the same	0.2 × 0.29 × D(urb)
Primary – Rescue/Emergency Medical	30% of fire density	0.3 × (0.29 × D(urb))	30% increase	1.3 × 0.29 × 0.5 × D(urb)
Rescue/EMS Civilian Support	20% of EMS density	0.2 × (0.3 × (0.29 × D(urb)	Remains the same	0.2 × 0.3 × 0.29 × D(urb)
Secondary – General Government and Civil Agencies	10% of police density	0.10 × D(urb)	Doubles	2.0 × 0.10 × D(urb)
Secondary – Volunteers and Other PPDR	5% of police density	0.05 × D(urb)	Doubles	2.0 × 0.05 × D(urb)

Example parameters

Narrowband – medium city – suburban – medium PPDR density

Population = 2 500 000 people
Area = 6 000 km^2
Police Density Suburban = U(sub) = 1.25 × 180 × 2 500 000/100 000 = 5 625 police
Cell radius = 14.4 km
Cell antenna pattern = Omni
Reuse factor = 21
GoS factor = 1.5
Width of frequency band = 24 MHz
Channel bandwidth = 12.5 kHz
% of band not used for traffic = 10%

Narrowband – medium city – urban – medium PPDR density

Population = 2 500 000 people
Area = 600 km^2
Police density suburban = U(urb) = 1.5 × 180 × 2 500 000/100 000 = 6 750 police
Cell radius = 5.0 km
Cell antenna pattern = Hex
Reuse factor = 21
GoS factor = 1.5
Width of frequency band = 24 MHz
Channel bandwidth = 12.5 kHz
% of band not used for traffic = 10%

Wideband – medium city – suburban – medium PPDR density

Population = 2 500 000 people
Area = 6 000 km^2
Police density suburban = U(sub) = 1.25 × 180 × 2 500 000/100 000 = 5 625 police
Cell radius = 9.2 km
Cell antenna pattern = Omni
Reuse factor = 12
GoS factor = 1.5
Width of frequency band = 24 MHz
Channel bandwidth = 150 kHz
% of band not used for traffic = 10%

Wideband – medium city – urban – medium PPDR density

Population = 2 500 000 people
Area = 600 km^2
Police density suburban = U(urb) = 1.5 × 180 × 2 500 000/100 000 = 6 750 police
Cell radius = 3.2 km
Cell antenna pattern = Hex
Reuse factor = 12
GoS factor = 1.5
Width of frequency band = 24 MHz
Channel bandwidth = 150 kHz
% of band not used for traffic = 10%

Narrowband – large city – suburban – medium PPDR density

Population = 8 000 000 people
Area = 8 000 km^2
Police density suburban = U(sub) = 1.25 × 180 × 8 000 000/100 000 = 18 000 police
Cell radius = 11.5 km
Cell antenna pattern = Omni
Reuse factor = 21
GoS factor = 1.5
Width of frequency band = 24 MHz
Channel bandwidth = 12.5 kHz
% of band not used for traffic = 10%

Narrowband – large city – urban – medium PPDR density

Population = 8 000 000 people
Area = 800 km^2
Police density suburban = U(urb) = 1.5 × 180 × 8 000 000/100 000 = 21 600 police
Cell radius = 4.0 km
Cell antenna pattern = Hex
Reuse factor = 21
GoS factor = 1.5
Width of frequency band = 24 MHz
Channel bandwidth = 12.5 kHz
% of band not used for traffic = 10%

Wideband – large city – suburban – medium PPDR density

Population = 8 000 000 people
Area = 8 000 km^2
Police density suburban = U(sub) = 1.25 × 180 × 8 000 000/100 000 = 18 000 police
Cell radius = 7.35 km
Cell antenna pattern = Omni
Reuse factor = 12
GoS factor = 1.5
Width of frequency band = 24 MHz
Channel bandwidth = 150 kHz
% of band not used for traffic = 10%

Wideband – large city – urban – medium PPDR density

Population = 8 000 000 people
Area = 800 km^2
Police density suburban = U(urb) = 1.5 × 180 × 2 500 000/100 000 = 21 600 police
Cell radius = 2.56 km
Cell antenna pattern = Hex
Reuse factor = 12
GoS factor = 1.5
Width of frequency band = 24 MHz
Channel bandwidth = 150 kHz
% of band not used for traffic = 10%

Annex 5

Existing and emerging solutions to support interoperability for public protection and disaster relief

1 Introduction

Interoperability is becoming increasingly important for PPDR operations. PPDR interoperability is the ability of PPDR personnel from one agency/organization to communicate by radio with personnel from another agency/organization, on demand (planned and unplanned) and in real time. There are several elements/components which affect interoperability including, spectrum, technology, network, standards, planning, and available resources. Regarding the technology element, there are a variety of solutions implemented either through pre-planning activities or by using particular technologies, which could support and facilitate interoperability.

A variety of these new technologies with future enhancements including developments in digital processing techniques, could be applied to increase the data throughput of systems supporting PPDR. These technologies could also support and may enable dissimilar radios to be interoperable across different frequency bands and with different waveforms. Current advanced solutions could also satisfy some PPDR requirements by assisting the migration to new technology solutions. This Annex provides a general description of some of the existing and emerging solutions which PPDR agencies and organizations could employ in combination with the other key elements (spectrum, standards, etc.) required to facilitate interoperability.

2 Existing solutions

Because of each administration's ability to adopt and implement different standards and policies, harmonizing frequency bands on a global/regional basis for future PPDR solutions may not satisfy full interoperability with either future or legacy equipment. The following solutions have historically been used to facilitate interoperability.

2.1 Cross-band repeaters

Although less spectrum efficient, the cross-band repeater solution may provide interoperability, especially on a temporary basis. It is a viable solution when agencies, which need to interoperate use different bands and have incompatible systems (either conventional or trunked communications systems, using analog versus digital modulation and operating in wideband versus narrowband mode). Currently, this solution is a practical approach for radio-radio interconnection because audio and push-to-talk (PTT) logic inputs and outputs are typically available. It requires little or no dispatcher involvement and is typically automated. Once activated, all broadcasts from one channel of one radio system are rebroadcast onto one channel of the second radio system. It also allows each user group involved to use its own subscriber equipment and allows subscriber equipment to have only basic features. The mobile radio implementation of cross-band repeaters is used, especially in mobile command vehicles, by public protection agencies to interconnect mobile users in different frequency bands. Using cross-banding repeaters is a method to solve spectrum and standards incompatibilities with a technology that exists today.

2.2 Radio reprogramming

Radio reprogramming to provide channel interoperability occurs between user groups operating in the same frequency band by allowing frequencies to be installed in all incident responders' radio equipment. Therefore, in order for this to be an effective solution, the radios should have this as a built-in capability. Radio reprogramming costs less than other interoperability solutions; it may or may not require additional infrastructure; it does not require coordinating and licensing of additional frequencies; and it can provide interoperability on very short notice. New techniques such as over the air reprogramming allow for instantaneous reprogramming to first responders in critical situations. This can be extremely useful in providing dynamic changes in a chaotic environment.

2.3 Radio exchange

Exchange of radios is a simple means to obtain interoperability. Radio exchange provides interoperability between responders with incompatible systems; it does not require coordinating and licensing of additional frequencies; and it can provide interoperability on very short notice.

2.4 Multi-band, multi-mode radios

Although the initial investment to purchase these radios is significant, it does provide several advantages:

– no dispatcher intervention is required;

– users can establish more than one simultaneous interoperability talk group or channel simply by having subscriber units switch to the proper frequency or operational mode;

– agencies need not change, reprogram, or add to the radio system infrastructure on any backbone systems;

– outside users can join the interoperability talk group(s) or channel(s) by simply selecting the right switch positions on their subscriber units; and

– no additional wireline leased circuits are needed. Multi-band, multi-mode radios can provide interoperability among subscriber units on the same radio system or on different systems. Equipment specifically designed and currently available that can operate on many frequency bands and in different voice and data modes. This also provides flexibility for users to operate independent systems in support of their missions with the added capability of linking different systems and bands on an as needed basis. Although this solution is not wide-spread due to the lack of software defined radios (SDRs), many public protection agencies use radios that operate in different frequency bands for interoperability.

SDR technology, for example, may permit interoperability without incurring other incompatibilities. The use of SDRs for commercial use, particularly for PPDR has potential advantages for meeting multiple standards, multiple frequencies, and the reduction of mobile and station equipment complexity.

2.5 Commercial services

The use of commercial services is effective in providing interoperability for by some extent PPDR organizations on an interim basis, particularly when administrative connectivity between disparate users is necessary. This interoperability solution is also beneficial in off loading administrative or non-critical communications when the demand for the tactical system is greatest.

2.6 Interface/interconnect systems

Although a substantial investment is required to purchase interface/interconnect systems, they have proven to be effective in providing interoperability between different communications systems. These systems can simultaneously cross-band two or more different radio systems such as HF, VHF, UHF, 800 MHz, trunking, and satellite; or connect a radio network to a telephone line or a satellite. The ability to interface/interconnect different systems allow the users of different equipment in different bands the ability to utilize the type of equipment that best meets their requirements.

3 Emerging technology solutions for PPDR

For solving future bandwidth requirements, there are several emerging technologies that may be applied to increase the data throughput of PPDR systems which may also reduce the amount of spectrum needed to support PPDR applications.

3.1 Adaptive antenna systems

Adaptive antenna systems could improve the spectral efficiency of a radio channel and, by so doing, greatly increase the capacity and coverage of most radio transmission networks. This technology uses multiple antennas, digital processing techniques and complex algorithms to modify the transmit and receive signals at the base station and at the user terminal. Commercial, private and government radio systems might obtain significant capacity and performance improvements from the application of adaptive antenna systems. The use of adaptive antenna systems in PPDR systems could increase the capacity of those networks within a limited bandwidth.

3.2 Cross-banding

Cross-banding is a solution that permits a radio operating on one frequency band to interoperate with another radio in a different frequency band is a technology that the PPDR community already uses and needs to use even more. Cross-banding can yield dividends because it permits operators to continue using existing frequencies and lets the translator do the work to accommodate the various users across different bands. If SDR technology is incorporated into the translator first, then legacy systems with their current waveforms can interoperate today, and these systems can be adaptable for tomorrow.

One other consideration with translators is the possibility of cross-moding, which could, for example, permit a UHF AM radio to interoperate with a UHF FM radio.

3.3 SDR

Enhanced functions for the user are possible with SDR technology that uses computer software to generate its operating parameters, particularly those involving waveforms and signal processing. This is currently in use by some government agencies. Some companies are also starting to benefit by using SDR technology in their products. SDR’s systems have the ability to span multiple bands and multiple modes of operation and will have the capability in the future to adjust its operating parameters, or reconfigure itself, in response to changing environmental conditions. An SDR radio will be able to electronically “scan” the spectrum to determine if its current mode of operation will permit it to operate in a compatible fashion with both legacy systems and other SDRs on a particular frequency in a particular mode. SDR systems could be capable of transmitting voice, video, and data, and have the ability to incorporate cross-banding which could allow for the ability to communicate, bridge, and route communications across dissimilar systems. Such systems could be remotely controlled, and may be compatible with new products and backward compatible with legacy systems. By building upon a common open architecture, this SDR system will improve interoperability by providing the ability to share waveform software between radios, even radios in different physical domains. Further, SDR technology could facilitate public protection organizations to operate in a harsh electromagnetic environment, to not be readily detected by scanners, and to be protected from interference by a sophisticated criminal element. Additionally, this system could replace a number of radios currently operating over a wide range of frequencies and allow interoperation with radios operating in disparate portions of that spectrum.

Annex 1: List of ITU-R Recommendations relating to telecommunications/ICT for disaster mitigation

RECOMMENDATION ITU-R M.693 – Technical characteristics of VHF emergency position-indicating radio beacons using digital selective calling (DSC VHF EPIRB)

RECOMMENDATION ITU-R M.830-1 – Operational procedures for mobile-satellite networks or systems in the bands 1 530-1544 MHz and 1 626.5-1 645.5 MHz which are used for distress and safety purposes as specified for the GMDSS

RECOMMENDATION ITU-R S.1001-1 – Use of systems in the fixed-satellite service in the event of natural disasters and similar emergencies for warning and relief operations

RECOMMENDATION ITU-R M.1042-3 – Disaster communications in the amateur and amateur-satellite services

RECOMMENDATION ITU-R F.1105-2 – Transportable fixed radiocommunications equipment for relief operations

RECOMMENDATION ITU-R M.1467-1 – Prediction of A2 and NAVTEX ranges and protection of A2 global maritime distress and safety system distress watch channel

RECOMMENDATION ITU-R M.1637 – Global cross-border circulation of radiocommunication equipment in emergency and disaster relief situations

RECOMMENDATION ITU-R M.1746 – Harmonized frequency channel plans for the protection of property using data communication

RECOMMENDATION ITU-R BT.1774 – Use of satellite and terrestrial broadcast infrastructures for public warning, disaster mitigation and relief

List of ITU-R Reports relating to Emergency Communications

REPORT ITU-R M.2033 – Radiocommunication objectives and requirements for public protection and disaster relief

VOLUME III

ITU-T CONTRIBUTION

TO THE COMPENDIUM OF ITU'S WORK

ON EMERGENCY TELECOMMUNICATIONS

TABLE OF CONTENTS

Page

Page

Introduction

1 ITU-T activities on Standardization for Emergency Telecommunications

Although ITU-T is not involved in emergency and disaster relief operations *per se*, it develops Recommendations that are fundamental to the implementation of interoperable systems and telecommunication facilities that will allow relief workers to smoothly deploy telecom equipment and services. Supplementary information material has also been produced by some of the study groups. In addition, substantial effort has been put into coordination and collaboration with other bodies, including the organization of workshops in 2002 and 2006.

1.1 Partnership Coordination Panel on TDR

In order to better support and coordinate its standardization work relating to emergency telecommunications, ITU-T has established a coordination group called the Partnership Coordination Panel on Telecommunications for Disaster Relief (PCT-TDR) as a follow-up action from the ITU-T Workshop on Telecommunications for Disaster Relief (Geneva, 17-19 February 2003; see www.itu.int/ITU-T/worksem/ets). The home page of this group is found at www.itu.int/ITU-T/special-projects/pcptdr.

The PCP-TDR gathers people working with standardization of telecommunication technologies for disaster relief (ITU, ISO, OASIS, etc.) and representatives of relief organizations, such as the United Nations High Commissariat for Refugees (UN-HCR), the UN Office for Coordination of Humanitarian Affairs (UN-OCHA), the International Federation of the Red Cross and Red Crescent (IFRC), and Télécoms Sans Frontières (TSF).

1.2 Technical documents for emergency telecommunications

A number of Recommendations have been developed for call priority schemes that ensure that relief workers can get communication lines when they need to. For example, E.106 defines the International Emergency Preference Scheme (IEPS), which aims to provide authorized emergency personnel a higher probability of successful communication using the PSTN under high network-load conditions, such as those that might occur in an emergency. There are also Recommendations that extend call priority to IP-based systems designed by ITU, such as H.323 and IPCablecom. Telecom network management in emergency situations is dealt with in M.3350, and a Framework for support of emergency communications in the Next Generation Network is found in Y.1271. A further Recommendation, Y.NGN-ET-Tech, on technical issues for emergency telecommunications in Next Generation Networks is being progressed by ITU-T Study Group 13. The intent is to fulfil the requirements and capabilities for emergency telecommunications as specified in Y.2201, indicating what features and mechanisms of an NGN may be used to facilitate the requirements of emergency telecommunications and early warning. ITU-T Study Group 11 is currently working on documents expressing the signalling requirements for Emergency Telecommunication Service (ETS) and for Telecommunication for Disaster Relief (TDR) in IP networks.

Complementary to the need to provide call priority during emergencies is the ability to deliver warnings to users. The new Recommendation H.460.21 provides a message broadcast mechanism in H.323 systems, which are widely deployed worldwide for Voice over IP (VoIP) communications. This mechanism is akin to that of Cell Broadcast for mobile systems and can be used by network operators and service providers to deliver early warning messages to a large number of users on an administrative domain without causing overload of the underlying network infrastructure. ITU-T Study Group 2 initiated work in February 2007 on possible standardization of numbering resources used for the GSM Cell Broadcast service. Additionally, ITU-T Study Group 17 has adopted the Common Alert Protocol (CAP) initially developed by OASIS as ITU-T Recommendation X.1303. The ITU-T Focus Group on IPTV has recently included in the draft IPTV service requirement specification the support for emergency alert services.

Enhancements were recently introduced in a number of multimedia system Recommendations to allow transparent signalling of IEPS call priority (H.225.0 and H.460.4). New E.107 concerning Emergency Telecommunications Service (ETS) and Interconnection Framework for National Implementations of ETS has been recently approved.

Additionally, ITU-T Study Group 2 has agreed to the allocation of a special country code to be managed by the United Nations Office for Coordination of Humanitarian Affairs (OCHA) for efficient communications in support of response efforts to disasters.

1.4 ITU-T Action Plan

ITU-T has also created an *ITU-T Action Plan for Standardization on Telecommunications for Disaster Relief and Early Warning (TDR/EW)*, motivated by the identification of the need for new telecommunication standards following the Indian Ocean tsunami of December 2004. The latest version can be found at www.itu.int/ITU-T/emergencytelecoms/plan-tdrew.html.

All study groups were encouraged to increase their activities in the definition of Recommendations and other materials (e.g. handbooks) on emergency telecommunications and to provide feedback to the Telecommunication Standardization Advisory Group (TSAG) and ITU-T Study Group 2 (which is to coordinate the effort) on actions taken and on proposals for improvement to the Action Plan.

2 Summary of ITU-T materials addressing emergency telecommunications

As of the date of publication of this compendium, the following are the ITU-T Recommendations that specifically address emergency telecommunications:

- ITU-T Rec. E.106, "International Emergency Preference Scheme (IEPS)" for disaster relief operations
- ITU-T Rec. E.107, "Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS"
- ITU-T Rec. X.1303, "Common alerting protocol (CAP 1.1)"
- ITU-T H.246 Amendment 1,"Mapping of user priority level and country/international network of call origination between H.225 and ISUP"
- ITU-T Rec. H.248.44, "Gateway control protocol: Multi-level precedence and pre-emption package"
- ITU-T Rec. H.460.4, "Call priority designation and country/international network of call origination identification for H.323 priority calls"

- ITU-T Rec. H.460.14, "Support for Multi-Level Precedence and Preemption (MLPP) within H.323 systems"
- ITU-T Rec. H.460.21 "Message broadcast for H.323 systems"
- ITU-T Rec. J.260, "Requirements for Preferential telecommunications over IPCablecom Networks"
- ITU-T Rec. M.3350, "TMN service management requirements for information interchange across the TMN X-interface to support provisioning of Emergency Telecommunication Service (ETS)"
- Signalling for IEPS support in ISUP: Q.761 Amd.3, Q.762 Amd.3, Q.763 Amd.4, and Q.764 Amd.4
- Signalling for IEPS support in BICC: Q.1902.1 Amd.2, Q.1902.2 Amd.3, Q.1902.3 Amd.3, and Q.1902.4 Amd.3
- Signalling for IEPS support in CBC: Q.1950 Amd.1 Annex G
- Signalling for IEPS support in ATM AAL2: Q.2630.3 Amd.1
- Signalling for IEPS support in DSS2: Q.2931 Amd.5
- ITU-T Rec. Y.1271, "Framework(s) on network requirements and capabilities to support emergency communications over evolving circuit-switched and packed-switched networks"

In addition to these Recommendations, there are two non-normative publications:

- Supplement 47 to ITU-T Q-series Recommendations, "Emergency services for IMT-2000 networks – Requirements for harmonization and convergence"
- Supplement 53 to ITU-T Q-series Recommendations, "Signalling requirements to support the International Emergency Preferential Scheme (IEPS)"

In the near future, it is expected that a number of new Recommendations and Supplements will be approved:

- Draft new ITU-T Rec. Y.NGN-ET-Tech, "Next Generation Networks – Emergency Telecommunications – Technical Considerations"
- Draft new ITU-T Rec. J.pref, "Specifications for preferential telecommunications over IPCablecom networks"
- Draft new ITU-T Rec. J.preffr, "Framework for implementing preferential telecommunications in IPCablecom networks"
- Draft new Supplements to the Q-series:
  - TRQ.ETS "Signalling requirements to support the Emergency Telecommunication Service (ETS) in IP networks"
  - TRQ.TDR "Signalling requirements to support the Telecommunication for Disaster Relief (TDR) in IP networks"

3 Challenges for the future

ITU-T has taken note of the report from the Second Phase of the World Summit on the Information Society (WSIS), in particular in §91 of the *Tunis Agenda for the Information Society* (concerning the important role of ICTs for disaster early warning, management and emergency communications) and the other relevant discussions. ITU-T will contribute to the international efforts aiming at implementing those requests.

ITU's overall strategy is to promote the use of ICT for multi-hazard preparedness, response and relief and to ensure that current efforts to establish early warning systems take into account the need for reliable telecommunications networks that provide a variety of channels of communication for the timely dissemination of information.

It is generally agreed that the most effective approach to telecommunication deployment should be highly focused, taking into account four distinct communication channels:

First, **citizen to authority**: ITU-T's focus here has been on providing last mile solutions. These are solutions that facilitate communications between citizens and authorities in times of emergency. For example, special numbers such as 911 in North America or 112 in Europe, which provide instant connections to emergency response teams. While this may provide some regulatory challenges, these can be overcome with conditions on telecommunication licensing.

Next, communications from **authority to authority**: Ways need to be found to facilitate communications between the national and international agencies involved in disaster management in order to maximize and coordinate relief efforts. For example, radio communications between police and fire brigades, and communications from field health workers to monitoring centres.

Thirdly, **authority to citizen**. This may be the most critical communication step of all, if citizens are to be warned of an impending disaster and to get instructions on what they should do. Radio and television broadcasts, Internet websites, and perhaps SMS / cell broadcast messages to mobile phones, can all play an important role here.

Finally, **citizen to citizen**: one must also address the social concerns of those in the affected regions, as well as the anxiety of their relatives who want information as to their health and safety. Again, radio and television, the Internet and mobile telephony are critical methods to address this need.

ITU-T will continue to pursue its core mission of delivering Recommendations that will allow systems developers to add, in an interoperable and consistent fashion, facilities to their systems that will be able to reliably respond to emergency situations.

In the context of standardization, it is necessary to define, together with relevant partners, the extensions or add-ons to enable emergency telecommunications in already deployed telecommunication systems and networks, such as PSTN, ISDN, and IP-based networks, solutions based on globally accepted standards. With regards to new systems such as NGN, they should have built-in features that natively support emergency telecommunications needs using globally defined telecommunications standards.

Concerning early warning systems, most of the issues faced in their design depend on existing systems, this requiring some system integration from the technical point of view. Issues such as types of sensors, location, information needed (i.e. sea bottom maps), models, etc, are usually well understood, but not yet well coordinated or elaborated. There are other issues that need to be taken into account, including understanding the hazards and traditional solutions at local level, dissemination, and capacity building. These have important telecommunications components, either from the infrastructure aspect or from the "tools" aspect (e.g. videoconferencing). In terms of standardization, these could lead to system-specific add-ons or framework recommendations. *The High-Level Expert Meeting on Technical Options for Disaster Management Systems: Tsunamis and Others*, UNESCAP, Bangkok, June 2005 recognized the importance to use true consensus-based international standards, as opposed to *lattu sensu* standards.

Even though outside of the scope of standardization work perse, appropriate regulatory frameworks are needed to facilitate the deployment and use of telecommunication equipment for disaster relief. While this is within the mandate of the ITU Development Sector, ITU-T is committed to contribute with its technical expertise when necessary.

As the Sector goes ahead with its standardization work, it will need support from members that can provide invaluable input of the general requirements and deployment scenarios.

In addition to its standardization activities, ITU-T will pursue promotion of awareness of its related deliverables, including the expected organization of future workshops involving key stakeholders. ITU-T will continue to cooperate with the relevant bodies – be it other SDOs, the many related intergovernmental organizations, NGOs, and Member States, in addition of course to ITU-D and ITU-R. For this, via the PCP-TDR, ITU-T intends to bring closer user groups that would not normally participate in our standards-setting process – as they have actual experience and will certainly contribute to the development of meaningful technical standards.

Service definition

ITU-T Rec. E.106 (10/2003)

INTERNATIONAL EMERGENCY PREFERENCE SCHEME (IEPS) FOR DISASTER RELIEF OPERATIONS

Summary

This Recommendation describes an international preference scheme for the use of public telecommunications by national authorities for emergency and disaster relief operations. The International Emergency Preference Scheme for Disaster Relief Operations (IEPS) is needed when there is a crisis situation causing an increased demand for telecommunications when use of the International Telephone Service may be restricted due to damage, reduced capacity, congestion or faults. In crisis situations there is a requirement for IEPS users of public telecommunications to have preferential treatment.

Introduction

In a crisis situation, there is a need for telecommunications among IEPS users of public telecommunications networks, such as the PSTN, ISDN or PLMN. These communications, which are regarded as essential, will be needed at the same time as the public will be attempting an increased number of calls during the period when the telecommunications networks may be restricted due to damage, congestion or faults.

Many countries have, or are developing, national preference schemes to allow preferential treatment for such national traffic. However, during a crisis, it is important for an international support scheme to allow communications between the IEPS users in one country and their correspondents in another. The International Emergency Preference Scheme for Disaster Relief Operations (IEPS) addresses this international support scheme.

This preference scheme is only intended for use by IEPS users to be able to place calls with preference. Public emergency services, on the other hand, are intended for use by members of the general public to request services such as fire, police, and medical. They are often invoked by a short access code.

1 Scope

The IEPS enables the use of public telecommunications by national authorities for emergency and disaster relief operations. It allows users, authorized by national authorities, to have access to the International Telephone Service, as described in ITU-T Rec. E.105 [1], while this service is restricted either due to damage, congestion or faults, or any combination of these. This Recommendation describes the functional requirements, features, access and the operational management of the IEPS.

2 References

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

[1] ITU-T Recommendation E.105 (1992), *International telephone service*.

3 Definitions

This Recommendation defines the following term:

3.1 IEPS user: User authorized by a national authority to have access to IEPS. The specific mechanism that a national authority uses to authorize a user is a national matter and is outside the scope of this Recommendation.

4 Abbreviations

This Recommendation uses the following abbreviations:

HPC	High Priority Call
IEPS	International Emergency Preference Scheme for Disaster Relief Operations
ISDN	Integrated Services Digital Network
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RNMC	Restrictive Network Management Control

5 Overall functional requirements

The primary goal for IEPS is to support crisis management arrangements. IEPS should significantly increase the ability of IEPS users to initiate and complete their communications (voice and data) via the PSTN, ISDN or PLMN irrespective of the bearer technology.

National preference schemes are intended for use in times of national crisis, but there could be occasions when an international preference scheme may need to be enabled while use of the respective national preference scheme would be unnecessary. An example of this is when intense international traffic is generated to a distant country in crisis. Therefore, international and national preference schemes need to be considered as independent and compatible.

IEPS users of a national preference scheme may not be eligible to gain access to the international scheme, but IEPS users of the international scheme should be able to use their own national preference scheme.

It is recognized that in some national systems, IEPS features may be permanently enabled.

IEPS users should be able to use their normal telecommunications equipment in times of crisis. When making an IEPS call, the PSTN/ISDN/PLMN should not appear markedly different to an IEPS user.

Calls originated by IEPS users should be given priority through the networks involved when IEPS is enabled.

Under conditions of severe damage or congestion, countries should be able to effect network controls, particularly over incoming traffic, even though IEPS may have been invoked.

In order to ensure that an IEPS user can reliably call any other telecommunications user, any restrictions to call completion should be overridden. This does not include pre-emption of any existing calls.

Access to public emergency services is not impacted by this Recommendation.

Countries may establish bilateral agreements with regard to the exchange of preference calls and the treatment of such calls.

Both the technical means and the management procedures for the initiation and operation of IEPS should be established and should be compatible with the existing national network traffic management schemes.

This preference scheme is only intended for use by IEPS users to be able to place calls with preference. Public emergency services, on the other hand, are intended for use by members of the general public to request services such as fire, police, and medical. They are often invoked by a short access code.

6 IEPS features

Calls from IEPS users should be suitably marked (see Note 1) at the network entrance and such markings should be associated with the call to completion (i.e., EPS calls should be marked from end to end).

NOTE 1 – **Call Marking**: A specific identifying mark is associated with the call which prompts operational elements of the public switched network to provide advantages in signalling, switching and traffic routing over non-marked calls. Call marking facilities are available in modern signalling networks and these can be used by the telecommunications providers to allow call completion advantages to preference user's calls.

NOTE 2 – The call marking, marking interpretation and the processing arrangements will have to be specified and fully agreed at the gateway points. Arrangements to transfer the marked signals would also need to be agreed with non-participating intermediate service providers of the transit networks.

The essential network features for the successful operation of IEPS are:

a) priority dial tone;

b) priority call setup, including priority queuing schemes; and

c) exemption from restrictive management controls, such as call gapping.

A list of features that will enhance call completion are mentioned in Annex A.

All IEPS calls will be of the same call class such that there will be only one level of priority for IEPS calls, however, some implementations may provide enhanced service features by analyzing additional signalling information provided by the call initiator. For example, the country of call origination may have a multi-level preference scheme and may make an agreement with the country of call destination for this multi-level preference scheme to be mapped onto that of the country of destination. In such circumstances it is essential that the information relating to level of priority be carried transparently across the international network and presented to the destination network. Transit networks not supporting the IEPS concept should not be required to examine the preference information but should simply pass the signalling information without any change.

Pre-emption in the Public Network (i.e., terminating any existing call) should not be provided.

7 Operational management of the IEPS

Requests for enabling the IEPS should be coordinated between the involved countries. In each country, IEPS will be authorized by the national authority and it will be their responsibility to establish the necessary arrangements.

IEPS users are to be determined by national authorities. Some criteria a national authority may wish to consider for the selection of IEPS users can be found in Appendix I.

To optimize the success of these calls there should be exemption from any restrictive network management controls. There should be preferential access to network resources. These preferential calls might also circumvent terminating user-invoked network features that might prevent alerting such as, for example, do not disturb or call screening.

If a network element is not able to respond to the preferential call request, the routing of the call should not be adversely affected, nor should any preference indicators be removed.

Annex A

Features and techniques to enhance call completion

The features described in this annex may be used separately or in combination to increase the probability of the successful completion of calls, but IEPS is not necessarily dependent on them. The list is not exclusive and the use of these features is to be determined by each country, taking into account the capabilities of the networks being used.

No.	Essential features for IEPS	Feature requires call marking
1	Priority dial tone – wireline or wireless connections (Essential Line service)	No
2	Priority call setup message through signalling network with high priority call identifier (HPC identifier)	Yes
3	Priority indicator in bearer networks	Yes
4	Exemption from restrictive network management controls, such as call gapping (Exemption from RNMC)	Yes

No.	Optional features (F) and techniques (T) to enhance call completion	Feature requires call marking
5	Survivable access and egress from end user location to PSTN/ISDN/PLMN: (F) a) Local exchange bypass; (T) b) Diverse PSTN/ISDN access from cellular; (T) c) Prescription override; (T) d) Avoidance routing; (T) e) Diverse routing. (T)	 Yes Yes Yes Yes Yes
6	IEPS user verification (F)	Yes
7	Special announcements on call progress (F)	Yes
8	Special routing capabilities: (F) a) Enhanced alternate routing; (T) b) Trunk queuing; (T) c) Off-hook trunk waiting; (T) d) Dynamic trunk reservation; (T) e) Trunk sub-grouping; (T) f) Automatic call rerouting; (T) g) PSTN/ISDN/PLMN partitioning. (T)	 Yes Yes Yes Yes Yes No No
9	Call forwarding (F)	Yes
10	Abbreviated dialling (F)	No
11	Attendant override (F)	Yes
12	Authorization codes (F)	No
13	Automatic call distribution (F)	No
14	Call-by-call service selection (F)	No
15	Call pickup (F)	No
16	Call transfer (F)	No
17	Call waiting (F)	No
18	Calling number identification (F)	No

A.1 Priority dial tone

This is a service arrangement that enhances the ability of IEPS users to receive priority over other users for the reception of dial tone. This is a restrictive treatment of non-IEPS users. Note that access denial systems are an extreme form of restrictive treatment by limiting dial tone to permitted lines only.

A.2 Priority call setup message through national and international signalling network with call identifier

This is a method of marking and identifying IEPS calls. As the IEPS call progresses through the networks, this identifier would enable special routing and preferential treatment to ensure the higher probability of call completion.

A.3 Priority indicator in bearer networks

This is a method of marking and identifying IEPS connection set ups and should cause priority allocation of bearer resources. As the IEPS connection set up progresses through the networks, this identifier could enable special routing and preferential treatment to ensure the higher probability of connection establishment. The preferential allocation of bearer resources should be maintained throughout the duration of the call.

A.4 Exemption from restrictive management controls

Network management is a set of control measures used to prevent or control degradation of network service. These measures are either expansive or protective. Expansive measures increase call routing choices by providing more capability than normal to carry excess traffic. Protective measures limit calls going into a switch or trunk group. An IEPS call should be exempt from restrictive controls, but should still benefit from expansive controls.

A.5 Survivable access and egress from end user location to PSTN/ISDN/PLMN

Techniques that enhance survivable access from the end user to the PSTN/ISDN/PLMN are described in a to e.

a) **Local exchange bypass**

The use of direct access services to, or egress services from, Switched Networks by using either bulk, wideband, switched, point-to-point, or circuit-by-circuit services. These services are available from providers such as cellular service providers, specialized service providers and satellite service providers.

b) **Diverse PSTN/ISDN access from PLMN**

This technique allows PLMNs to directly interconnect with other elements of PSTN/ISDN. This allows PLMN calls to be routed around failed or congested nodes. Network access diversity allows specifically identified calls to be routed to private or special purpose networks.

c) **Prescription override**

The ability to select an alternative carrier, e.g., by dialling a specific code or operating a selection key on the terminal instrument, or may be automatic for an IEPS call.

d) **Avoidance routing**

This technique, with limited availability, permits a user to enhance their survivability in PSTN/ISDN by directing the service provider to assign them to transmission facilities that avoid points of vulnerability such as earthquake zones or hurricane areas.

e) **Diverse routing**

This technique provides the user with a second route over physically separate facilities, which can be used if the primary route is unavailable.

A.6 IEPS user verification

This feature allows for the verification of the IEPS user. Personal Identification Numbers (PINs), line identification, authorization codes or call-back facilities could be used to verify the call as an authorized IEPS call.

A.7 Special announcements on call progress

This feature will provide recorded voice announcements to the user when calls cannot be completed or to provide problem and restoration information.

A.8 Special routing capabilities

Special routing capabilities that enhance call completion are described in a to g.

a) **Enhanced alternate routing**

Routing programs are used to provide special routing controls and paths within a network.

b) **Trunk queuing**

This technique would hold the IEPS call in queue until a trunk became available, then the first call in queue (the IEPS call) would have access to the next available trunk. The IEPS call would not receive an immediate "all trunks busy" tone.

c) **Off-hook trunk waiting**

This technique allows the IEPS caller to remain off-hook and the network continually searches, at predetermined intervals (i.e., several seconds) for an idle trunk if no idle trunk was found on the initial attempt.

d) **Dynamic trunk reservation**

This technique automatically reserves reservation of trunks for certain classes of calls under designated conditions. It could be implemented or activated in the following ways:

– IEPS calls could be allocated a variable number of trunks between switches according to demand;
– the use of network management control under predetermined conditions, to reserve trunks in an idle condition for the exclusive use of IEPS calls; and
– the designation of specific sub-groups within a trunk group that, under predetermined conditions, would be reserved for IEPS calls.

e) **Trunk sub-grouping**

This technique splits trunks into pre-assigned sub-groups; one for general use and another for IEPS use only. Under normal conditions, general use traffic could use either sub-group. During emergencies, only IEPS calls would use the IEPS sub-group. Overflow from the IEPS sub-group could be routed over the general use sub-group but the general calls would not be allowed to overflow to the IEPS sub-group.

f) **Automatic call rerouting**

This technique allows calls to be routed over other operator's networks.

g) **PSTN/ISDN/PLMN partitioning**

This is the use of hardware or software to separate traffic into specific functional groups for the purpose of providing special service capabilities such as enhanced call completion for IEPS calls.

A.9 Call forwarding

This feature enables calls to be rerouted automatically from one line to another, or to an attendant.

A.10 Abbreviated dialling

A feature by which a user can attempt a call by dialling a two- or three-digit code that instructs a database to obtain the actual desired number from a look-up table and transmit it into the network to connect the calling line to the called line.

A.11 Attendant override

A feature that allows the terminal equipment operator to interrupt a call that is in progress.

A.12 Authorization codes

Unique multi-digit codes used to allow an IEPS user privileged access to a network, system or device. If the code is validated the call is allowed to advance.

A.13 Automatic call distribution

A system designed to evenly distribute traffic by directing incoming calls over a group of terminals.

A.14 Call-by-call service selection

A feature that provides improved trunking efficiency between end-user location and end-office by allowing a variety of services to use the same trunk group and by distributing traffic over the total number of available trunks on a call-by-call basis.

A.15 Call pickup

This feature enables a connected extension to answer any ringing extension within an assigned call pickup group.

A.16 Call transfer

A feature whereby a call to a user's number is automatically transferred to one or more alternative numbers when the called number is busy or does not answer.

A.17 Call waiting

A feature that provides a distinctive audible tone to a busy user's line to notify the user when another caller is attempting to reach his/her number.

A.18 Calling number identification

A feature that provides the identification of the calling user's number by means of a visual or audible identification at the called terminal.

Appendix I

Criteria for the selection of IEPS users

IEPS users are to be determined by their national authorities. The criteria for selection that a national authority may wish to consider are listed as, but are not limited to, the following items:

- civil defense/"home defense", e.g., public warning systems;
- diplomatic and other vital governmental purposes;
- state security purposes including customs and immigration;
- emergency services by local authorities, including police, fire services, etc.;
- posts and telecommunications service providers, for maintaining their service provision to other essential users;
- public utilities including energy, water supplies, etc.;
- medical services;
- air and sea rescue.

ITU-T Rec. E.107 (02/2007)

EMERGENCY TELECOMMUNICATIONS SERVICE (ETS) AND INTERCONNECTION FRAMEWORK FOR NATIONAL IMPLEMENTATIONS OF ETS

Summary

There is a potential for bilateral/multilateral agreement between cooperating countries/administrations to link their respective Emergency Telecommunications Service (ETS) systems. This Recommendation provides guidance that will enable telecommunications between one ETS national implementation (ENI) and another ENI, in addition to providing a description of ETS.

Introduction

Countries have, or are developing, ETSs. Implementation of ETS by definition is a national matter. However, disasters/emergencies can transcend geographic boundaries, and thus there is a potential that countries/administrations may enter into bilateral and/or multilateral agreements to link their respective ETS systems. This Recommendation provides guidance that will enable telecommunications between one ETS national implementation (ENI) and other ENI(s).

1 Scope

This Recommendation provides guidance that will enable telecommunications between one ETS national implementation (ENI) and other ENI(s) (authority-to-authority), in addition to providing a description of ETS.

Early warning (EW) for disasters is not part of this Recommendation, but is left for future studies that may add to this Recommendation or become a separate Recommendation.

2 References

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

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

3 Definitions

This Recommendation defines the following terms:

3.1 Emergency Telecommunications Service (ETS): A national service providing priority telecommunications to the ETS authorized users in times of disaster and emergencies.

3.2 ETS user: A user authorized to obtain priority telecommunications in national and/or international emergency situations.

3.3 priority treatment capabilities: Capabilities that provide priority in the use of telecommunications network resources, allowing a higher probability of end-to-end telecommunications and use of telecommunication applications.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ENI	ETS National Implementation
ETS	Emergency Telecommunications Service
IEPS	International Emergency Preference Scheme
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
NGN	Next Generation Network
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SIP	Session Initiation Protocol
TDM	Time Division Multiplex
TDR	Telecommunications for Disaster Relief
UDP	User Datagram Protocol

5 Conventions

None.

6 Emergency telecommunications service

ETS is a national implementation utilizing the features, facilities and applications available in national public networks and service offerings. As such, it could be said to resemble a supplementary service since it can only exist if there is an established telecommunication service. Implementation of ETS by definition is a national matter; however, ETS national implementations are likely to exhibit some of the following characteristics:

a) ETS users should be able to use their normal telecommunication terminals to initiate ETS calls, sessions or telecommunication during times of crisis or agreed emergency situations.

b) An originating national network may use various methods to identify an ETS user request for ETS telecommunication.

c) As a national capability, ETS is specifically designed to serve the telecommunication needs of authorized ETS users. How ETS users are authenticated and authorized is a national matter.

d) An ETS call, session or telecommunication is provided end-to-end priority treatment beyond that offered to the general public. The priority treatment is applied during the call/session establishment phase, and should continue to be applied for the duration of the call, session or telecommunication. The priority treatment consists of priority mechanisms and features applicable to various aspects (e.g., signalling, control, routing, and media traffic) that are essential for the establishment and continuation of the telecommunication, including:

- **Priority treatment**: Priority treatment mechanisms may include priority call/session set-up (e.g., priority queuing schemes for network resources), access to additional resources (e.g., via alternate routing) and exemption from restrictive network traffic management controls (e.g., call gapping). Pre-emption in the public network (i.e., terminating any established telecommunication to release resources to serve a new ETS call/session request) is a national matter.

- **Network interconnection and protocol interworking**: The signalling of ETS indicators transmitted across network boundaries (e.g., between a circuit-switched network and an NGN, etc.) and the ETS priority treatment should also be ensured to be interoperable across the relevant networks.

e) An ETS user should be able to communicate with any other available user. For example, any restrictions to call/session completion should be overridden.

f) A national government/administration decides whether user priority levels will be assigned to ETS users, and if assigned, how many levels will be used and the assignment criteria.

g) If a network or network element is not able to distinguish an ETS call/session request from a normal call request, then the routing of an ETS requested call should proceed as a normal call and any ETS markings or indicators associated with the call should be maintained and transmitted if technically feasible.

7 ENI-to-ENI interconnection

Countries have, or are developing, ETSs to allow priority treatment for authorized traffic to support emergency and disaster relief operations within their national boundaries. However, there could be a crisis situation where it is important for an ETS user in one country to communicate with available users in another country. In this case, it is important for an ETS call/session originated in one country to receive end-to-end priority treatment, i.e., priority treatment in the originating country and the destination country. This may require interconnection of two ETS national implementations via an international network that provides priority treatment capabilities. The term gateway in the following guidelines should be interpreted to be a traditional gateway exchange in a circuit-switched network or an equivalent for NGN networks. The following provides guidance for such an interconnection:

a) Countries may establish bilateral/multilateral agreements with regard to the exchange and treatment of ETS calls, sessions and telecommunications. Even though ETS may have been invoked, national authorities should be able to retain control of network management functions for their own telecommunication networks, including those elements relating to international traffic with other countries.

b) An outgoing international gateway shall provide priority treatment to an ETS call, session or other telecommunication. It will provide, if necessary, appropriate mapping of the originating country's national ETS indicators to the corresponding international call markings so that the ETS call, session or other telecommunication receives priority treatment in the international network. As this ETS call, session, or other telecommunication proceeds through the international network to an incoming international gateway, the incoming international gateway shall also provide priority treatment. It will provide, if necessary, appropriate mapping of the international call markings associated with the ETS call, session, or other telecommunication to the corresponding national indicators of the destination country so that the ETS call, session or other telecommunication receives priority treatment in the destination country.

c) Based on bilateral/multilateral agreement between countries/administrations, the information relating to the ETS user priority level shall be carried transparently across the international network and presented to the destination network. The incoming gateway in the destination country may provide a mapping of the ETS user priority level received from the originating country to that of the country of call/session destination.

d) If a transit network is not able to distinguish an ETS call/session request from a normal call/session request, then the ETS call/session request should be processed as a normal call/session request and any international call markings associated with the call/session should be passed without change.

e) TDR facilities may be used, based on bilateral/multilateral agreement between countries/ administrations, for interconnection of ETS national implementations, for example, thereby supporting international calls, sessions or telecommunication between ETS national systems. The international emergency preference scheme (IEPS) for disaster relief operations described in [ITU-T E.106] provides priority treatment for international telephony services 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.

f) Based on bilateral/multilateral agreement between countries/administrations, mobility of ETS users shall be supported.

ITU-T Rec. Y.1271 (10/2004)

FRAMEWORK(S) ON NETWORK REQUIREMENTS AND CAPABILITIES TO SUPPORT EMERGENCY COMMUNICATIONS OVER EVOLVING CIRCUIT-SWITCHED AND PACKED-SWITCHED NETWORKS

Summary

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

1 Introduction

The purpose of emergency telecommunications is to facilitate emergency recovery operations with the goal for restoring the community infrastructure and for returning the population to normal living conditions after serious disasters. Responders need to assess the damage, coordinate rescue and medical assistance, harmonize restoration endeavours, etc. For supporting this purpose, emergency telecommunications may be provided through shared resources from the public telecommunications infrastructure that is evolving from a basic circuit-switched to packet-switched networks with a variety of telecommunication capabilities.

2 Scope

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

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

3 References

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

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

4 Definitions

This Recommendation defines the following terms:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.15 **preferential**: A capability offering advantage over regular capabilities.

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

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

5 Abbreviations

This Recommendation uses the following abbreviations:

QoS Quality of Service

SLA Service Level Agreement

6 Security

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

7 Consideration

7.1 The nature of emergency situations

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

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

7.2 Emergency response

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

The common thread to facilitate operations for all disaster recovery phases is the utility of fast, reliable, user-friendly emergency telecommunications that may be realized by technical solutions and/or administrative policy.

7.3 Assured telecommunications

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

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

The affiliation of an emergency worker may be known in advance of an actual emergency situation. In this case, their credentials may be stored thereby allowing the person to be authenticated for an authorized telecommunication. Generally, when preferential or priority treatment telecommunication capabilities are offered, users of the service should be authorized. Whether authorization is required shall be national matters of the respective particular country. However, without authorization, preferential treatment capabilities may be subject to abuse by non-authorized individuals.

Circuit-switched networks respond to overload situations by denying call attempt when resources are saturated. One option is to pre-empt other callers when authorized emergency communication workers need to communicate. However, some types of networks respond to an additional load by degrading performance of the entire network. This occurs when networks operate under a best-effort framework where all information is treated the same and simply queued or dropped until network resources are available.

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

8 Emergency telecommunications requirements and capabilities

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

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

Table 1 provides objectives and functional requirements.

Table 1/Y.1271 – Emergency telecommunications functional requirements and capabilities

Enhanced priority treatment
Secure networks
Location Confidentiality
Restorability
Network connectivity
Interoperability
Mobility

Table 1/Y.1271 – Emergency telecommunications functional requirements and capabilities *(end)*

Ubiquitous coverage
Survivability/endurability
Voice transmission
Scaleable bandwidth
Reliability/availability

8.1 Enhanced priority treatment

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

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

8.1.1 Preferential access to telecommunications facilities

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

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

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

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

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

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

8.1.3 Preferential routing of emergency telecommunication traffic

In some situations, emergency traffic could be redirected to alternate paths when default paths have become unusable or congested. In evolving networks, it is desirable for emergency telecommunications to avoid single points of failure and hence possibly have multiple backup paths or alternate routing for use during periods of overload or failed connections through the network. In packet-based networks, routing of packets is a continuing process for an instance of telecommunication until the session has reached completion.

8.1.4 Optional pre-emption of non-emergency traffic

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

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

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

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

8.2 Secure networks

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

8.2.1 Rapid authentication of authorized users for emergency telecommunications

The emergency telecommunications is intended only for authorized users who participate in emergency recovery operations. The appropriate authority of each nation or community may authorize these designated users. Upon initiation of an emergency communication request, for evolving networks, it is desirable to request to establish an innovative method for a streamlined rapid user authentication process in these evolving telecommunication networks, including mobile networks which verifies the user's identity to protect the telecommunication resources against excessive use and abuse during an emergency situation. Once an authentication is validated and emergency telecommunication travels across networks, such authentication information may be associated with labels that then should be transported from the call initiation until termination. It may be necessary for the label to remain throughout the duration of the emergency call.

8.2.2 Security protection of emergency telecommunication traffic

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

8.3 Location confidentiality

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

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

8.4 Restorability

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

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

8.5 Network connectivity

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

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

In certain liberalized and competitive environments, there may be:

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

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

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

8.6 Interoperability

Evolving networks will produce a number of issues, one of which is to ensure orderly and transparent continuance of the basic ITU-T Rec. E.106 emergency preference capabilities. During the convergence period, the different schemes for interworking between the circuit-switched and packet-switched technologies need to be considered. For example, voice calls from the telephone or mobile network may transit packet-switched networks and then terminate in either the circuit-switched network or directly in a packet-switched network. Interworking preferential treatment methods over heterogeneous networks needs to be addressed.

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

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

8.7 Mobility

Mobility calls for a telecommunications infrastructure that is integrated with transportable, re-deployable, and fully mobile facilities. In order to have mobile capabilities, a common configuration provides key elements to facilitate capabilities for emergency applications. The telecommunications infrastructure should support user and terminal mobility including re-deployable, or fully mobile telecommunications.

8.8 Ubiquitous coverage

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

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

8.9 Survivability/endurability

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

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

8.10 Voice transmission

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

8.11 Scaleable bandwidth

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

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

8.12 Reliability/availability

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

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

Annex A/Y.1271

A possible distinction between essential and optional requirements

Emergency communications functional requirements and capabilities	Description	Essential	Optional
Enhanced priority treatment	Emergency traffic needs assured capabilities regardless of the networks traversed.	X	
Secure networks	Networks should have protection against corruption of, or unauthorized access to, traffic and control (fraud), including expanded encryption techniques and user authentication, as appropriate.	X	
Location Confidentiality	A limited number of high level leadership emergency telecommunication users may need to be able to use emergency telecommunications without risk of being located.		X
Restorability	Certain network functionalities should be capable of being reprovisioned, repaired, or restored to required levels on a priority basis.		X
Network connectivity	Networks supporting emergency telecommunications should provide international connectivity when possible, e.g., when **ITU-T Rec. E.106 is applicable.**	X	
Interoperability	Provide interconnection and Interoperability among all networks (evolving or existing).	X	
Mobility	The telecommunications infrastructure should support user and terminal mobility including re-deployable, or fully mobile telecommunications.		X
Ubiquitous coverage	Public telecommunication infrastructure resources over large geographic areas should form the framework for ubiquitous coverage of emergency telecommunications.	X	
Survivability/endurability	Capabilities should be robust to support surviving users under a broad range of circumstances.	X	
Voice transmission	Circuit-switched and packet-switched networks need to provide voiceband quality service for emergency telecommunications users.	X	
Scaleable bandwidth	Authorized users should be able to select the capabilities of emergency telecommunications to support variable bandwidth requirements.		X
Reliability/availability	Telecommunications should perform consistently and precisely according to their design requirements and specifications, and should be usable with high confidence.	X	

Appendix I/Y.1271

Information on possible sources of disasters

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

Typically, natural disasters often set off additional clamorous events. For example, a hurricane may induce flash floods and mudslides. Hurricanes may cause rivers to overflow resulting in the death of livestock or damaged crops. People can be left without electricity or homes leaving them in need of food, clothing and shelter. Earthquakes continue to create damage after the initial quake through aftershocks. Sometimes earthquakes induce tidal waves that inflict additional damage to an already affected area. Some natural disasters are presented below.

Table I.1/Y.1271 – Natural disasters

Avalanches
Drought
Earthquakes
Epidemics
Flash floods
Famine
Floods
Forest fires
Lightning
Hurricanes
Mudslides
Severe Cold, Snow, Ice or Heat
Tidal waves
Tornados
Tsunamis
Typhoons
Volcano eruptions
Wind storms

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

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

Table I.2/Y.1271 – Human-made disasters

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

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

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

Informative Supplement 47 to ITU-T Q Series – Recommendations (11/2003)

EMERGENCY SERVICES FOR IMT-2000 NETWORKS – REQUIREMENTS FOR HARMONIZATION AND CONVERGENCE

Summary

This Supplement is an "information" document and is intended to outline the requirements and provisions for Emergency Services for IMT-2000 systems. This is a compilation from sources outside the ITU (e.g., administrations, Standards Development Organizations, and the Third Generation Partnership Projects (3GPP and 3GPP2)). The scope includes any relevant discussion concerning the provisioning of Emergency Services specifically addressing the IMT-2000 systems during Harmonization and Convergence periods.

1 Scope

ITU-T Rec. Q.1701 provides the framework for IMT-2000 networks and defines the IMT-2000 Family of Systems concept. This Recommendation identified the following Emergency call capabilities to be supported on IMT-2000 systems:

- Identification of emergency call;
- Emergency call handling;
- Emergency caller location.

This Supplement to the Q-series of Recommendations identifies and discusses the requirements and provisioning of Emergency Services in IMT-2000 systems. For the purposes of this Supplement, Emergency Services include supporting national emergency calls and the International Emergency Preference Scheme (IEPS), as found in ITU-T Rec. E.106.

2 References

Excerpts from the following ITU-T Recommendations were used in this Supplement. The references below contain provisions which, through reference in this text, constitute provisions of this Supplement. At the time of publication, the editions indicated were valid. All Recommendations and the bibliographic references are subject to revision; users of this Supplement are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below and throughout the Supplement. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks*.

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

[3] ETSI SR 002 180 (2003), *Requirements for communication of citizens with authorities/organizations in case of distress (emergency call handling)*.

[4] 3GPP TR 22.950 (2003), *Priority service feasibility study* (Release 6).

[5] 3GPP TS 22.101 (2003), *Service aspects; Service principles* (Release 6).

[6] ITU-T Recommendation Q.767 (1991), *Application of the ISDN User Part of CCITT signalling system No. 7 for international ISDN interconnections* plus Amendment 1 (1991): *Support for the International Emergency Preference Scheme*.

[7] ITU-T Recommendations Q.1902.X series (2001), *Bearer Independent Call Control protocol (Capability Set 2),* plus Amendments.

[8] ITU-T Recommendations Q.761-Q.764 (1999), *Signalling System No. 7 – ISDN User Part,* plus Amendments.

[9] ITU-T Recommendations Q.2761-Q.2764 (1999), *Broadband ISDN User Part,* plus Amendments.

[10] ITU-T Recommendation Q.1950 (2002), *Bearer independent call control protocol*.

[11] TIA/ATIS, J-STD-034 (1997), *Wireless Enhanced Emergency Services*.

[12] TIA/ATIS, J-STD-036-A, (2002), *Enhanced Wireless 9-1-1 Phase 2*, and Addendum 1 (2003).

[13] Supplement 1 to ITU-T E.300-series Recommendations (1988), *List of possible supplementary telephone services which may be offered to subscribers*.

3 Definitions

This Supplement defines the following terms:

3.1 emergency call: A call requesting emergency services. A caller is given a fast and easy means of giving information about an emergency situation to the appropriate emergency organization (e.g. fire department, police, ambulance). Emergency calls will be routed to the emergency services in accordance with national regulations.

3.2 IEPS call: Allows an authorized user to have access to the International Telephone Service while the service is restricted due to damage, congestion and/or other faults. The International Emergency Preference Scheme (IEPS) is needed when there is a crisis situation, which causes abnormal telecommunication requirements for governmental, military, civil authorities and other specially authorized users of public telecommunication networks.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations:

3G	3rd Generation Wireless Systems
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
BICC	Bearer Independent Call Control
B-ISDN	Broadband ISDN
CS-2, CS-3	Capability Set 2, Capability Set 3
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile communications
IEPS	International Emergency Preference Scheme
IMT-2000	International Mobile Telecommunications-2000
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part

ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
SDO	Standards Development Organization

5 Introduction

IMT-2000 Family Members are third generation (3G) mobile systems that will provide access, by means of one or more radio links, to a wide range of telecommunication services supported by the fixed telecommunication networks, and to other services that are specific to mobile users.

This Supplement provides a high-level overview of Emergency Service Requirements for IMT-2000 systems, with particular attention to the period of harmonization and convergence.

6 Emergency calls

Emergency calls provide a means to contact authorities/organizations in all types of emergencies. It is a national matter to provide this important and fundamental capability to its citizens. However, with the global nature of IMT-2000 systems, there exists a need to identify and discuss the generic requirements to ensure these are met during the period of harmonization and convergence.

National regulatory authorities define the requirements for emergency calls (including location information). Future (harmonized/converged) IMT-2000 systems should contain the requisite technical capability to meet national requirements.

6.1 General emergency call requirements for IMT-2000 systems

It should always be possible for any terminal connected to a network to make an emergency call. A user must also be able to make an emergency call from a terminal that has been barred (e.g., because of non-payment of bills), that is protected by a password, and that does not have a User Identity Module (UIM), if it is not installed, or if it is not activated. Lastly, a user must be able to make an emergency call regardless of which operator is providing network coverage, as long as the user's terminal is technically compatible with the network operator's facilities in that area. Emergency calls should be identified as such (i.e., by means of identifying "emergency flag") by the network.

Emergency calls should be possible regardless of any terminal equipment feature that might conceivably prevent the emergency call from being initiated. Emergency calls should also be possible in case of mains power failure.

Any emergency call, as well as IEPS calls by authorized users (see clause 7), should have precedence over regular phone calls in case of network overload.

Emergency calls must be routed to the appropriate emergency centre, in accordance with national regulations. This also applies if the call transits a different network between originating and terminating networks or if networks belong to different operators. If possible, there should be a clear and unambiguous mapping between the caller's location and the emergency centre responsible for the appropriate area. All precautions should be taken to avoid losing or misrouting any emergency call.

Emergency calls should be protected against possible attempts to obstruct or otherwise impede the provision, operation and performance of the emergency call service. Deployment of the end-to-end integrity and traceability of the origin of the call and the identity of the caller should be considered.

6.2 Specific harmonization and convergence emergency call requirements

Each network must be able to recognize emergency calls. The originating network must generate the emergency call-related information (i.e., the originating telephone number, if available, and location of the calling party, as available) and make this information available to the emergency centre. The generation and transmission of this information shall not unduly delay the transmission of the emergency call. So far as possible/practical, each IMT-2000 system shall present as accurate as technically feasible location information to the emergency call handling answering point, in a common format.

With the global roaming capability, users should be able to make an emergency call using the appropriate invocation sequence, even if that invocation is different from their home network's method.

7 International Emergency Preference Scheme (IEPS)

ITU-T Rec. E.106 describes an International Emergency Preference Scheme (IEPS) that allows authorized users to have access to the International Telephone Service while the service is restricted due to damage, congestion and/or other faults. IEPS provides these authorized users a significant increase in their ability to initiate and complete their communications (voice and data) via the PSTN, ISDN, and PLMN.

IEPS calls are identified and marked at the network entrance and this marking should be associated with the call to completion. The essential network features are priority dial tone, priority call set-up, including priority queuing schemes, and exemption from restrictive network management controls.

7.1 Overview of IEPS requirements in IMT-2000

Administrations will determine their requirements for their own national preference schemes. However, despite the independency of international and national preference schemes, they should be compatible.

IEPS calls should be protected against possible attempts to obstruct or otherwise impede the provision, operation and performance of the IEPS service. Deployment of end-to-end integrity and an authentication mechanism for IP-based communications should be considered. Providing confidentiality for IEPS call traffic should also be considered.

7.2 Specific harmonization and convergence IEPS requirements

The ITU-T Recommendations supporting ISUP-2000 (ITU-T Recs Q.761-Q.764), B-ISDN, (ITU-T Recs Q.2761-Q.2764), and BICC (ITU-T Recs Q.1902.1-Q.1902.4, and Q.1950) have been amended to support IEPS. ITU-T Rec. Q.767 was also amended to provide support for IEPS. IMT-2000 systems interfacing with the International Telephone System should, at a minimum, carry the IEPS marker (a specific calling party category) transparently.

Alert messaging

ITU-T Rec. X.1303 (09/2007) – Prepublished version

COMMON ALERTING PROTOCOL (CAP 1.1)

Summary

The common alerting protocol (CAP) is a simple but 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.

This Recommendation also provides both an XSD specification and an equivalent ASN.1 specification (that permits a compact binary encoding) and allows the use of ASN.1 as well as XSD tools for the generation and processing of CAP messages. This Recommendation enables existing systems, such as H.323 systems, to more readily encode, transport and decode CAP messages.

Introduction

This clause provides a brief introduction to the Common Alerting Protocol (The current specification is identified as CAP 1.1).

1 Purpose

The common alerting protocol (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;
- Compatible with digital encryption and signature capability; and,
- Facility for digital images and audio.

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

2 CAP History

The National Science and Technology Council report on "Effective Disaster Warnings" released in November, 2000 recommended that "a standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally and nationally for input into a wide variety of dissemination systems."

An international working group of more than 130 emergency managers and information technology and telecommunications experts convened in 2001 and adopted the specific recommendations of the National Science and Technology Council (NSTC) report as a point of departure for the design of a Common Alerting Protocol (CAP). Their draft went through several revisions and was tested in demonstrations and field trials in Virginia (supported by the ComCARE Alliance) and in California (in cooperation with the California Office of Emergency Services) during 2002 and 2003.

Geographic locations in CAP are defined using [b-WGS 84] (World Geodetic System 1984). CAP does not assign responsibilities for coordinate transformations from and to other Spatial Reference Systems. See clause 5, below, for the format of coordinate pairs within CAP elements.

In 2002, the CAP initiative was endorsed by the national non-profit Partnership for Public Warning, which sponsored its contribution in 2003 to the OASIS standards process. In 2004, CAP version 1.0 was adopted as an OASIS Standard.

3 Structure of the CAP Alert Message

Each CAP Alert Message consists of an <alert> segment, which may contain one or more <info> segments, each of which may include one or more <area> segments. Under most circumstances, CAP messages with a <msgType> value of "Alert" should include at least one <info> element. (See the document object model diagram in clause 7.1, below.)

- **<alert>**

The <alert> segment provides basic information about the current message: its purpose, its source and its status, as well as a unique identifier for the current message and links to any other related messages. An <alert> segment may be used alone for message acknowledgements, cancellations or other system functions, but most <alert> segments will include at least one <info> segment.

- **<info>**

The <info> segment describes an anticipated or actual event in terms of its urgency (time available to prepare), severity (intensity of impact) and certainty (confidence in the observation or prediction), as well as providing both categorical and textual descriptions of the subject event. It may also provide instructions for an appropriate response by message recipients and various other details (hazard duration, technical parameters, contact information, links to additional information sources, etc.). Multiple <info> segments may be used to describe differing parameters or to provide the information in multiple languages.

- **<resource>**

The <resource> segment provides an optional reference to additional information related to the <info> segment within which it appears, in the form of a digital asset such as an image or audio file.

- **<area>**

The <area> segment describes a geographic area to which the <info> segment in which it appears applies. Textual and coded descriptions (such as postal codes) are supported, but the preferred representations use geospatial shapes (polygons and circles) and an altitude or altitude range, expressed in standard latitude / longitude / altitude terms in accordance with a specified geospatial datum.

4 Applications of the CAP Alert Message

The primary use of the CAP Alert Message is to provide a single input to activate all kinds of alerting and public warning systems. This reduces the workload associated with using multiple warning systems while enhancing technical reliability and target-audience effectiveness. It also helps ensure consistency in the information transmitted over multiple delivery systems, another key to warning effectiveness.

A secondary application of CAP is to normalize warnings from various sources so they can be aggregated and compared in tabular or graphic form as an aid to situational awareness and pattern detection.

Although primarily designed as an interoperability standard for use among warning systems and other emergency information systems, the CAP Alert Message can be delivered directly to alert recipients over various networks, including data broadcasts. Location-aware receiving devices could use the information in a CAP Alert Message to determine, based on their current location, whether that particular message was relevant to their users.

The CAP Alert Message can also be used by sensor systems as a format for reporting significant events to collection and analysis systems and centers.

ITU-T Recommendation X.1303

COMMON ALERTING PROTOCOL (CAP 1.1)

1 Scope

This Recommendation defines the common alerting protocol (CAP) – version 1.1 – which is a simple but 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 facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

The common alerting protocol (CAP) provides an open, non-proprietary digital message format for various types of alerts and notifications. CAP provides the following capabilities:

- 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;
- Compatible with digital encryption and signature capability; and,
- Facility for digital images and audio.

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

This Recommendation also provides both an XSD schema and an ASN.1 specification for the common alerting protocol.

NOTE – The ASN.1 specification defines the same message information content and XML encoding as that defined by the XSD schema, but permits a compact binary encoding and the use of ASN.1 as well as XSD tools for the generation and processing of CAP messages.

This Recommendation is technically equivalent and compatible with the OASIS Common Alerting Protocol, v. 1.1. This Recommendation defines the following:

1) structure of the CAP alert message;
2) design principles and concepts of CAP;
3) alert message structure;
4) XML and compact binary encodings of the message (using XSD for the XML encoding and the ASN.1 specification and its Encoding Rules for the XML – identical to the XSD specification – and the binary encodings);
5) Conversion between compact binary and XML encodings of the message using ASN.1 Recommendations.

2 References

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

The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations. The IETF RFC-Editor maintains a list of RFCs, together with those that have been obsoleted by later RFCs. W3C and National Institute for Standards and Technology maintain a list of latest recommendations and other publications.

[ITU-T X.680] ITU-T Recommendation X.680, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[ITU-T X.691] ITU-T Recommendation X.691, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).*

[ITU-T X.693] ITU-T Recommendation X.693, *Information technology – ASN.1 encoding rules: Specification of XML Encoding Rules (XER).*

[ITU-T X.694] ITU-T Recommendation X.694, *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*.

[FIPS 180-2:2002] National Institute for Standards and Technology, Secure Hash Standard, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf, August 2002.

[IETF RFC 2046:1996] Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, IETF RFC, 1996.

[IETF RFC 3066:2001] Tags for the Identification of Languages, IETF RFC, 2001.

[W3C Datatypes:2004] XML Schema Part 2: Data types Second Edition, W3C Recommendation, Copyright © [24 October 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xmlschema-2/#dateTime.

[W3C Encryption:2002] XML Encryption Syntax and Processing, W3C Recommendation, Copyright © [10 December 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.

[W3C Namespaces:1999] Namespaces in XML, W3C Recommendation, Copyright © [14 January 1999] World Wide Web Consortium (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-xml-names/.

[W3C Signature:2002] XML Signature Syntax and Processing, W3C Recommendation, Copyright © [2 February 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xmldsigcore/.

[W3C XML:2004] Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-xml/.

3 Definitions

This clause is intentionally left blank.

4 Abbreviations and acronyms

ASN.1	Abstract Syntax Notation One
CAP	Common Alerting Protocol
EAS	Weather radio and the Emergency Alert System
MIME	Multipurpose Internet Mail Extensions
SAME	Specific Area Message Encoding
URI	Uniform Resource Identifier
XML	Extensible Markup Language
XSD	XML Schema Definition

5 Conventions

The words *warning*, *alert* and *notification* are used interchangeably throughout this document.

The term “coordinate pair” is used in this document to refer to a comma-delimited pair of decimal values describing a geospatial location in degrees, in the form “[latitude],[longitude]”. Latitudes in the Southern Hemisphere and longitudes in the Western Hemisphere are signed negative by means of a leading dash.

References to XML elements within the body of this Recommendation are in bold font.

6 Design principles and concepts

This clause is non-normative.

This clause provides a brief review of the design concepts and principles behind CAP.

6.1 Design Philosophy

Among the principles which guided the design of the CAP Alert Message were:

- Interoperability: First and foremost, the CAP Alert Message should provide a means for interoperable exchange of alerts and notifications among all kinds of emergency information systems.
- Completeness: The CAP Alert Message format should provide for all the elements of an effective public warning message.
- Simple implementation: The design should not place undue burdens of complexity on technical implementers.
- Simple XML (see [W3C XML:2004], [W3C Namespaces:1999], [W3C Datatypes:2004]) and portable structure: Although the primary anticipated use of the CAP Alert Message is as an XML document or its binary equivalent, the format should remain sufficiently abstract to be adaptable to other coding schemes.

- Multi-use format: One message schema supports multiple message types (e.g., alert / update / cancellations / acknowledgements / error messages) in various applications (actual / exercise / test / system message).
- Familiarity: The data elements and code values should be meaningful to warning originators and non-expert recipients alike.
- Interdisciplinary and international utility: The design should allow a broad range of applications in public safety and emergency management and allied applications and should be applicable worldwide.

6.2 Examples of Requirements for Design

Note – The following requirements were used as a basis for design and review of the CAP Alert Message format. This list is non-normative and not intended to be exhaustive.

The Common Alerting Protocol should:

- Provide a specification for a simple, extensible format for digital representation of warning messages and notifications;
- Enable integration of diverse sensor and dissemination systems;
- Be usable over multiple transmission systems, including TCP/IP-based networks and one-way "broadcast" channels and low-bandwidth communication;
- Support credible end-to-end authentication and validation of all messages;
- Provide a unique identifier (e.g., an ID number) for each warning message and for each message originator;
- Provide for multiple message types, such as:
  - Warnings,
  - Acknowledgements,
  - Expirations and cancellations,
  - Updates and amendments,
  - Reports of results from dissemination systems,
  - Administrative and system messages;
- Provide for multiple message types, such as:
  - Geographic targeting,
  - Level of urgency,
  - Level of certainty,
  - Level of threat severity;
- Provide a mechanism for referencing supplemental information (e.g., digital audio or image files, additional text);
- Use an established open-standard data representation;
- Be based on a program of real-world cross-platform testing and evaluation;
- Provide a clear basis for certification and further protocol evaluation and improvement; and,
- Provide a clear logical structure that is relevant and clearly applicable to the needs of emergency response and public safety users and warning system operators.

6.3 Examples of Use Scenarios

This sub-clause provides examples of use scenarios that were used as a basis for the design and review of the CAP Alert Message format.

Note – These scenarios are non-normative and not intended to be exhaustive or to reflect actual practices.

6.3.1 Manual Origination

"The Incident Commander at an industrial fire with potential of a major explosion decides to issue a public alert with three components:

a) An evacuation of the area within half a mile of the fire;

b) a shelter-in-place instruction for people in a polygon roughly describing a downwind dispersion "plume" extending several miles downwind and half a mile upwind from the fire; and

c) a request for all media and civilian aircraft to remain above 2500 feet above ground level when within a half mile radius of the fire.

"Using a portable computer and a web page (and a pop-up drawing tool to enter the polygon) the Incident Commander issues the alert as a CAP message to a local alerting network."

6.3.2 Automated Origination by Autonomous Sensor System

"A set of automatic tsunami warning sirens has been installed along a popular Northwest beach. A wireless network of sensor devices collocated with the sirens controls their activation. When triggered, each sensor generates a CAP message containing its location and the sensed data at that location that is needed for the tsunami determination. Each siren activates when the combination of its own readings and those reported at by other devices on the network indicate an immediate tsunami threat. In addition, a network component assembles a summary CAP message describing the event and feeds it to regional and national alerting networks."

6.3.3 Aggregation and Correlation on Real-time Map

"At the State Operations Center a computerized map of the state depicts, in real time, all current and recent warning activity throughout the state. All major warning systems in the state – the Emergency Alert System, siren systems, telephone alerting and other systems – have been equipped to report the details of their activation in the form of a CAP message. (Since many of them are now activated by way of CAP messages, this is frequently just a matter of forwarding the activation message to the state center.)

"Using this visualization tool, state officials can monitor for emerging patterns of local warning activity and correlate it with other real time data (e.g., telephone central office traffic loads, 9-1-1 traffic volume, seismic data, automatic vehicular crash notifications, etc.)."

6.3.4 Integrated Public Alerting

"As part of an integrated warning system funded by local industry, all warning systems in a community can be activated simultaneously by the issuance by authorized authority of a single CAP message.

"Each system converts the CAP message data into the form suitable for its technology (text captioning on TV, synthesized voice on radio and telephone, activation of the appropriate signal on sirens, etc.). Systems that can target their messages to particular geographic areas implement the targeting specified in the CAP message with as little 'spill' as their technology permits.

"In this way, not only is the reliability and reach of the overall warning system maximized, but citizens also get corroboration of the alert through multiple channels, which increases the chance of the warning being acted upon."

6.3.5 Repudiating a False Alarm

"Inadvertently the integrated alerting network has been activated with an inaccurate warning message. This activation comes to officials' attention immediately through their own monitoring facilities (e.g., 5.3.3 above). Having determined that the alert is, in fact, inappropriate, the officials issue a cancellation message that refers directly to the erroneous prior alert. Alerting systems that are still in the process of delivering the alert (e.g., telephone dialing systems) stop doing so. Broadcast systems deliver the cancellation message. Other systems (e.g., highway signs) simply reset to their normal state."

7 Alert Message Structure

This clause discusses CAP alert message structure.

7.1 Document Object Model

The CAP document object model is provided in Figure 6.1 below.

Note – In the Figure below, elements in boldface are mandatory; elements in italics have default values that will be assumed if the element is not present; asterisks (*) indicate that multiple instances are permitted.

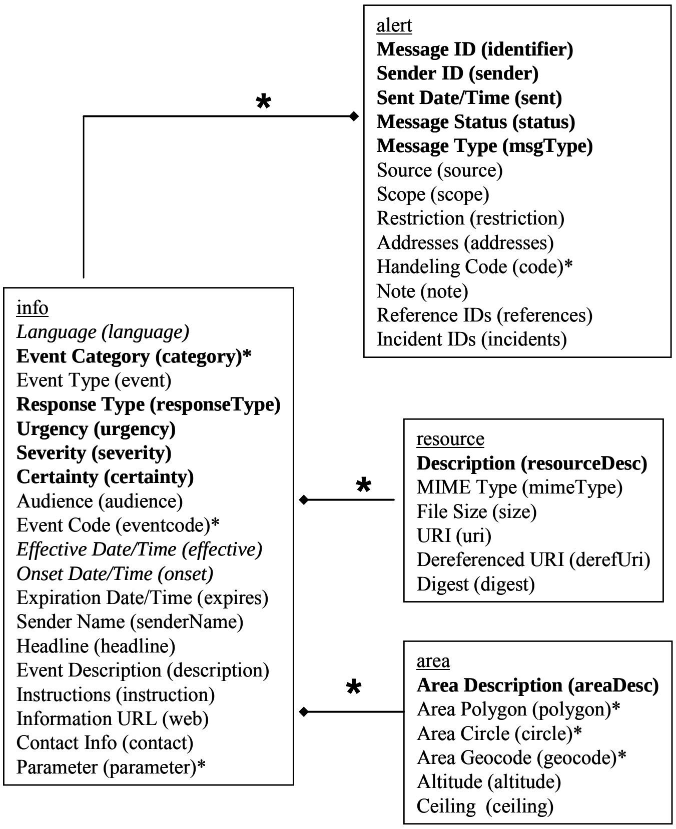


Figure 6.1 – Document Object Model

7.2 Data Dictionary

This sub-clause provides a description of the CAP data dictionary.

Note – Unless explicitly constrained within this Data Dictionary or the XML Schema (see [W3C XML:2004] and sub-clause 6.4), CAP elements may have null values. Implementers must check for this condition wherever it might affect application performance.

7.2.1 "alert" Element and Sub-elements

Table 6.1 provides a description of the "alert" element and sub-elements.

Table 6.1 – "alert" element and sub-elements

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
alert	**cap. alert. group**	**The container for all Component parts of the alert message (REQUIRED)**	(1) Surrounds CAP alert message subelements (2) Must include the xmlns attribute referencing the CAP URN as the namespace, e.g.: <cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1"> *[sub-elements]* </cap:alert> (3) In addition to the specified subelements, may contain one or more <info> blocks.
identifier	**cap. alert. identifier**	**The identifier of the alert message (REQUIRED)**	(1) A number or string uniquely identifying this message, assigned by the sender (2) Must not include spaces, commas or restricted characters (< and &)
sender	**cap. alert. sender. identifier**	**The identifier of the sender of the alert message (REQUIRED)**	(1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name (2) Must not include spaces, commas or restricted characters (< and &)
sent	**cap. alert. sent. time**	**The time and date of the origination of the alert message (REQUIRED)**	(1) The date and time is represented in [dateTime] format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at16: 49 PDT). (2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "–00:00" or "+00:00.
status	**cap. alert. status. code**	**The code denoting the Appropriate handling of the alert message (REQUIRED)**	Code Values: "Actual" – Actionable by all targeted recipients "Exercise"– Actionable only by designated exercise participants; exercise identifier should appear in <note> "System" – For messages that support alert network internal functions. "Test" – Technical testing only, all recipients disregard "Draft" – A preliminary template or draft, not actionable in its current form.

Table 6.1 – "alert" element and sub-elements *(cont.)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
msgType	**cap. alert. type. code**	**The code denoting the nature of the alert message (REQUIRED)**	Code Values: "Alert" – Initial information requiring attention by targeted recipients "Update" – Updates and supercedes the earlier message(s) identified in <references> "Cancel" - Cancels the earlier message(s) identified in <references> "Ack" – Acknowledges receipt and acceptance of the message(s)) identified in <references> "Error" indicates rejection of the message(s) identified in <references>; explanation should appear in <note>
source	cap. alert. source. identifier	The text identifying the source of the alert message (OPTIONAL)	The particular source of this alert; e.g., an operator or a specific device.
scope	cap. alert. scope. code	The code denoting the Intended distribution of the alert message (REQUIRED)	Code Values: "Public" – For general dissemination to unrestricted audiences "Restricted" – For dissemination only to users with a known operational requirement (see <restriction>, below) "Private" – For dissemination only to specified addresses (see <address>, below)
restriction	cap. alert. restriction. text	The text describing the rule for limiting distribution of the restricted alert message (conditional)	Used when <scope> value is "Restricted"
addresses	cap. alert. addresses. group	The group listing of Intended recipients of the private alert message (conditional)	(1) Used when <scope> value is "Private" (2) Each recipient shall be identified by an identifier or an address (3) Multiple space-delimited addresses may be included. Addresses including whitespace must be enclosed in double-quotes.
code	cap. alert. code	The code denoting the Special handling of the alert message (OPTIONAL)	(1) Any user-defined flag or special code used to flag the alert message for special handling. (2) Multiple instances may occur within a single <info> block.
note	cap. alert. note. text	The text describing the purpose or significance of the alert message (OPTIONAL)	The message note is primarily intended for use with Cancel and Error alert message types.
references	cap. alert. references. group	The group listing Identifying earlier message(s) referenced by the alert message (OPTIONAL)	(1) The extended message identifier(s) (in the form *sender,identifier,sent)* of an earlier CAP message or messages referenced by this one. (2) If multiple messages are referenced, they shall be separated by whitespace.

Table 6.1 - "alert" element and sub-elements *(end)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
incidents	cap. alert. incidents. group	The group listing naming the referent incident(s) of the alert message (OPTIONAL)	(1) Used to collate multiple messages referring to different aspects of the same incident (2) If multiple incident identifiers are referenced, they shall be separated by whitespace. Incident names including whitespace shall be surrounded by double-quotes

7.2.2 "info" Element and Sub-elements

Table 6.2 provides a description of the "info" element and sub-elements.

Table 6.2 – "info" element and sub-elements

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
info	cap. alertInfo. info. group	The container for all component parts of the info sub-element of the alert message (OPTIONAL)	(1) Multiple occurrences are permitted within a single <alert>. If targeting of multiple "info" blocks in the same language overlaps, information in later blocks may expand but may not override the corresponding values in earlier ones. Each set of "info" blocks containing the same language identifier shall be treated as a separate sequence. (2) In addition to the specified subelements, may contain one or more <resource> blocks and/or one or more <area> blocks.
language	cap. alertInfo. language. code	The code denoting the languag of the info subelement of the alert message (OPTIONAL)	(1) Code Values: Natural language identifier per [IETF RFC 3066:2001]. (2) If not present, an implicit default value of "en-US" shall be assumed. (3) A null value in this element shall be considered equivalent to "en-US."
category	**cap. alertInfo. category. code**	**The code denoting the category of the subject event of the alert message (REQUIRED)**	(1) Code Values: "Geo" – Geophysical (inc. landslide) "Met" – Meteorological (inc. flood) "Safety" – General emergency and public safety "Security" – Law enforcement, military, homeland and local/private security "Rescue" – Rescue and recovery "Fire" – Fire suppression and rescue "Health" – Medical and public health "Env" – Pollution and other environmental "Transport" – Public and private transportation

Table 6.2 - "info" element and sub-elements *(cont.)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
			"Infra" – Utility, telecommunication, other non-transport infrastructure "CBRNE" – Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack "Other" – Other events (2) Multiple instances may occur within a single <info> block.
event	**cap. alertInfo. event. text**	**The text denoting the type of the subject event of the alert message (REQUIRED)**	
responseType	cap. alertInfo. responseType. code	The code denoting the type of action recommended for the target audience (OPTIONAL)	(1) Code Values: "Shelter" – Take shelter in place or per <instruction> "Evacuate" – Relocate as instructed in the <instruction> "Prepare" – Make preparations per the <instruction> "Execute" – Execute a pre-planned activity identified in <instruction> "Monitor" – Attend to information sources as described in <instruction> "Assess" – Evaluate the information in this message. (This value should NOT be used in public warning applications.) "None" – No action recommended (2) Multiple instances may occur within a single <info> block.
urgency	**cap. alertInfo. urgency. code**	**The code denoting the urgency of the subject event of the alert message (REQUIRED)**	(1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. (2) Code Values: "Immediate" – Responsive action should be taken immediately "Expected" – Responsive action should be taken soon (within next hour) "Future" – Responsive action should be taken in the near future "Past" – Responsive action is no longer required "Unknown" – Urgency not known
severity	**cap. alertInfo. severity. code**	**The code denoting the severity of the subject event of the alert message (REQUIRED)**	(1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. (2) Code Values: "Extreme" – Extraordinary threat to life or property "Severe" – Significant threat to life or property "Moderate" – Possible threat to life or property "Minor" – Minimal threat to life or property "Unknown" – Severity unknown

Table 6.2 – "info" element and sub-elements *(cont.)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
certainty	**cap. alertInfo. certainty. code**	**The code denoting the certainty of the subject event of the alert message (REQUIRED)**	(1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. (2) Code Values: "Observed" – Determined to have occurred or to be ongoing. "Likely" - Likely (p > ~50%) "Possible" - Possible but not likely (p <=~50%) "Unlikely" - Not expected to occur (p ~ 0) "Unknown" - Certainty unknown (3) For backward compatibility with CAP 1.0, the deprecated value of "Very Likely" should be treated as equivalent to "Likely."
audience	cap. alertInfo. audience. text	The text describing the intended audience of the alert message (OPTIONAL)	
eventCode	cap. alertInfo. event. code	A systemspecific code identifying the event type of the alert message (OPTIONAL)	(1) Any system-specific code for event typing, in the form: <eventCode> <valueName>valueName</valueName> <value>value</value> </eventCode> where the content of "valueName" is a userassigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CEM"). (2) Values of "valueName" that are acronyms should be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). (3) Multiple instances may occur within a single <info> block.
effective	cap. alertInfo. effective. time	The effective time of the information of the alert message (OPTIONAL)	(1) The date and time is represented in [dateTime] format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at16: 49 PDT). (2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "–00:00" or "+00:00. (3) If this item is not included, the effective time shall be assumed to be the same as in <sent>.
onset	cap. alertInfo. onset. time	The expected time of the beginning of the subject event of the alert message (OPTIONAL)	(1) The date and time is represented in [dateTime] format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16: 49 PDT). (2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "–00:00" or "+00:00.

Table 6.2 – "info" element and sub-elements *(cont.)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
expires	cap. alertInfo. expires. time	The expiry time of the information of the alert message (OPTIONAL)	(1) The date and time is represented in [dateTime] format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). (2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "–00:00" or "+00:00. (3) If this item is not provided, each recipient is free to set its own policy as to when the message is no longer in effect.
senderName	cap. alertInfo. sender. name	The text naming the originator of the alert message (OPTIONAL)	The human-readable name of the agency or authority issuing this alert.
headline	cap. alertInfo. headline. text	The text headline of the alert message (OPTIONAL)	A brief human-readable headline. Note that some displays (for example, short messaging service devices) may only present this headline; it should be made as direct and actionable as possible while remaining short. 160 characters may be a useful target limit for headline length.
description	cap. alertInfo. description. text	The text describing the subject event of the alert message (OPTIONAL)	An extended human readable description of the hazard or event that occasioned this message.
instruction	cap. alertInfo. instruction. text	The text describing the recommended action to be taken by recipients of the alert message (OPTIONAL)	An extended human readable instruction to targeted recipients. (If different instructions are intended for different recipients, they should be represented by use of multiple <info> blocks.)
web	cap alertInfo. information. identifier	The identifier of the hyperlink associating additional information with the alert message (OPTIONAL)	A full, absolute URI for an HTML page or other text resource with additional or reference information regarding this alert
contact	cap. alertInfo. contact. text	The text describing the contact for follow-up and confirmation of the alert message (OPTIONAL)	
parameter	cap. alertInfo. parameter. group	A systemspecific additional parameter associated with the alert message (OPTIONAL)	(1) Any system-specific datum, in the form: <parameter> <valueName>valueName</valueName> <value>value</value> </parameter>

Table 6.2 - "info" element and sub-elements *(end)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
			where the content of "valueName" is a user-assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CIV".) (2) Values of "valueName" that are acronyms should be represented in all capital letters without periods (e.g., SAME,FIPS, ZIP). (3) Multiple instances may occur within a single <info> block.

7.2.3 "resource" Element and Sub-elements

Table 6.3 provides a description of the "resource" element and sub-elements.

Table 6.3 – "resource" element and sub-elements

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
resource	cap alertInfoResource. resource. group	The container for all Component parts of the resource subelement of the info subelement of the alert element (OPTIONAL)	(1) Refers to an additional file with supplemental information related to this <info> element; e.g., an image or audio file (2) Multiple occurrences may occur within a single <info> block
resourceDesc	**cap. alertInfoResource. resourceDesc. text**	**The text describing the type and content of the resource file (REQUIRED)**	The human-readable text describing the content and kind, such as "map" or "photo," of the resource file.
mimeType	cap. alertInfoResource. mimeType. identifier	The identifier of the MIME content type and sub-type describing the resource file (OPTIONAL)	MIME content type and sub-type as described in [IETF RFC 2046:1996]. (As of this document, the current IANA registered MIME types are listed at http://www.iana.org/assignments/mediatypes/)
size	cap. alertInfoResource. size. integer	The integer indicating the size of the resource file (OPTIONAL)	Approximate size of the resource file in bytes.
uri	cap. alertInfoResource. uri. identifier	The identifier of the hyperlink for the resource file (OPTIONAL)	A full absolute URI, typically a Uniform Resource Locator that can be used to retrieve the resource over the Internet OR a relative URI to name the content of a <derefUri> element if one is present in this resource block.

Table 6.3 – "resource" element and sub-elements *(end)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
derefUri	cap alertInfoResource. derefUri. data	The base-64 encoded data content of the resource file (conditional)	(1) may be used either with or instead of the <uri> element in messages transmitted over one-way (e.g., broadcast) data links where retrieval of a resource via a URI is not feasible. (2) Clients intended for use with one-way data links must support this element. (3) This element must not be used unless the sender is certain that all direct clients are capable of processing it. (4) If messages including this element are forwarded onto a two-way network, the forwarder must strip the <derefUri> element and should extract the file contents and provide a <uri> link to a retrievable version of the file. (5) Providers of one-way data links may enforce additional restrictions on the use of this element, including message-size limits and restrictions regarding file types.
digest	cap. alertInfoResource. digest. code	The code representing the digital digest ("hash") computed from the resource file (OPTIONAL)	Calculated using the Secure Hash Algorithm (SHA-1) per [FIPS 180-2:2002] Note – It should be noted that NIST is encouraging the use of SHA-256 as a more secure alternative to SHA-1.

7.2.4 "area" Element and Sub-elements

Table 6.4 provides a description of the "area" element and sub-elements.

Table 6.4 – "area" element and sub-elements

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
area	cap. alertInfoArea. area. group	The container for all component parts of the area subelement of the info subelement of the alert message (OPTIONAL)	
areaDesc	**cap. alertInfoArea. area. text**	**The text describing the affected area of the alert message (REQUIRED)**	A text description of the affected area.
polygon	cap. alertInfoArea. polygon. group	The paired values of points defining a polygon that delineates the affected area of the alert message (OPTIONAL)	(1) Code Values: The geographic polygon is represented by a whitespace-delimited list of coordinate pairs. Note – See 5.2. (2) The first and last pairs of coordinates must be the same.

Table 6.4 – "area" element and sub-elements *(cont.)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
			(3) See Coordinate Precision Note at end of this clause. (4) Multiple instances may occur within an <area>.
circle	cap. alertInfoArea. circle. group	The paired values of a point and radius delineating the affected area of the alert message (OPTIONAL)	(1) Code Values: The circular area is represented by a central point given as a coordinates pair followed by a space character and a radius value in kilometers. Note – per the [b-WGS 84] datum, see 5.2. (2) See Coordinate Precision Note at end of this clause. (3) Multiple instances may occur within an <area>.
geocode	cap. alertInfoArea. geocode. code	The geographic code delineating the affected area of the alert message (OPTIONAL)	(1) Any geographically-based code to describe message target area: <parameter> <valueName>valueName</valueName> <value>value</value> </parameter> where the content of "valueName" is a userassigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="006113"). (2) Values of "valueName" that are acronyms should be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). (3) Multiple instances may occur within a single <info> block. (4) This element is primarily for compatibility with other systems. Use of this element presumes knowledge of the coding system on the part of recipients; therefore, for interoperability, it should be used in concert with an equivalent description in the more universally understood <polygon> and <circle> forms whenever possible.

Table 6.4 – "area" element and sub-elements *(end)*

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
altitude	cap. alertInfoArea. altitude. quantity	The specific or minimum altitude of the affected area of the alert message (OPTIONAL)	(1) If used with the <ceiling> element this value is the lower limit of a range. Otherwise, this value specifies a specific altitude. (2) The altitude measure is in feet above mean sea level. Note – per the [b-WGS 84] datum, see 5.2.
ceiling	cap. alertInfoArea. ceiling. quantity	The maximum altitude of the affected area of the alert message (conditional)	(1) Must not be used except in combination with the <altitude> element (2) The ceiling measure is in feet above mean sea level. Note – per the [b-WGS 84] datum, see 5.2.

7.3 Implementation Considerations

This sub-clause defines some insights into CAP implementations.

7.3.1 Security

Because CAP is an XML-based format, existing XML security mechanisms can be used to secure and authenticate its content. While these mechanisms are available to secure CAP Alert Messages, they should not be used indiscriminately.

This sub-clause adds two tags to CAP by reference. These are: "Signature and "EncryptedData". Both elements are children of the <alert> element and are optional. If the "EncryptedData" element exists, no other elements will be visible until after the message is decrypted. This makes the minimal CAP message an alert element which encloses an EncryptedData element. The maximal CAP message, if an EncryptedData element is present is an <alert> element enclosing a single EncryptedData element and a single Signature element.

7.3.2 Digital Signatures

The alert element of a CAP Alert Message may have an Enveloped Signature, as described by XML-Signature and Syntax Processing (see [W3C Signature:2002]). Other XML signature mechanisms must not be used in CAP Alert Messages.

Processors must not reject a CAP Alert Message containing such a signature simply because they are not capable of verifying it; they must continue processing and may inform the user of their failure to validate the signature.

In other words, the presence of an element with the namespace URI (see [W3C Signature:2002]) and a local name of "Signature" as a child of the alert element must not cause a processor to fail merely because of its presence.

7.3.3 Encryption

The alert element of a CAP Alert Message may be encrypted, using the mechanisms described by XML Encryption Syntax and Processing (see [W3C Encryption:2002]). Other XML encryption mechanisms must not be used in CAP Alert Messages; however, transport-layer encryption mechanisms may be used independently of this requirement.

7.4 XML Schema

```
<?xml version = "1.0" encoding = "UTF-8"?>
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
   targetNamespace = "urn:oasis:names:tc:emergency:cap:1.1"
   xmlns:cap = "urn:oasis:names:tc:emergency:cap:1.1"
   xmlns:xs = "http://www.w3.org/2001/XMLSchema"
   elementFormDefault = "qualified"
   attributeFormDefault = "unqualified">
  <element name = "alert">
    <annotation>
      <documentation>CAP Alert Message (version 1.1)</documentation>
    </annotation>
    <complexType>
      <sequence>
        <element name = "identifier" type = "string"/>
        <element name = "sender" type = "string"/>
        <element name = "sent" type = "dateTime"/>
        <element name = "status">
          <simpleType>
            <restriction base = "string">
              <enumeration value = "Actual"/>
              <enumeration value = "Exercise"/>
              <enumeration value = "System"/>
              <enumeration value = "Test"/>
              <enumeration value = "Draft"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "msgType">
          <simpleType>
            <restriction base = "string">
              <enumeration value = "Alert"/>
              <enumeration value = "Update"/>
              <enumeration value = "Cancel"/>
              <enumeration value = "Ack"/>
              <enumeration value = "Error"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "source" type = "string" minOccurs = "0"/>
        <element name = "scope">
          <simpleType>
            <restriction base = "string">
              <enumeration value = "Public"/>
              <enumeration value = "Restricted"/>
              <enumeration value = "Private"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "restriction" type = "string" minOccurs = "0"/>
        <element name = "addresses" type = "string" minOccurs = "0"/>
        <element name = "code" type = "string" minOccurs = "0" maxOccurs =
"unbounded"/>
        <element name = "note" type = "string" minOccurs = "0"/>
        <element name = "references" type = "string" minOccurs = "0"/>
        <element name = "incidents" type = "string" minOccurs = "0"/>
        <element name = "info" minOccurs = "0" maxOccurs = "unbounded">
          <complexType>
            <sequence>
              <element name = "language" type = "language" default = "en-US"
minOccurs = "0"/>
              <element name = "category" maxOccurs = "unbounded">
                <simpleType>
                  <restriction base = "string">
                    <enumeration value = "Geo"/>
```

```
                    <enumeration value = "Met"/>
                    <enumeration value = "Safety"/>
                    <enumeration value = "Security"/>
                    <enumeration value = "Rescue"/>
                    <enumeration value = "Fire"/>
                    <enumeration value = "Health"/>
                    <enumeration value = "Env"/>
                    <enumeration value = "Transport"/>
                    <enumeration value = "Infra"/>
                    <enumeration value = "CBRNE"/>
                    <enumeration value = "Other"/>
                  </restriction>
                </simpleType>
              </element>
              <element name = "event" type = "string"/>
              <element name = "responseType" minOccurs = "0" maxOccurs =
"unbounded">
                <simpleType>
                  <restriction base = "string">
                    <enumeration value = "Shelter"/>
                    <enumeration value = "Evacuate"/>
                    <enumeration value = "Prepare"/>
                    <enumeration value = "Execute"/>
                    <enumeration value = "Monitor"/>
                    <enumeration value = "Assess"/>
                    <enumeration value = "None"/>
                  </restriction>
                </simpleType>
              </element>
              <element name = "urgency">
                <simpleType>
                  <restriction base = "string">
                    <enumeration value = "Immediate"/>
                    <enumeration value = "Expected"/>
                    <enumeration value = "Future"/>
                    <enumeration value = "Past"/>
                    <enumeration value = "Unknown"/>
                  </restriction>
                </simpleType>
              </element>
              <element name = "severity">
                <simpleType>
                  <restriction base = "string">
                    <enumeration value = "Extreme"/>
                    <enumeration value = "Severe"/>
                    <enumeration value = "Moderate"/>
                    <enumeration value = "Minor"/>
                    <enumeration value = "Unknown"/>
                  </restriction>
                </simpleType>
              </element>
              <element name = "certainty">
                <simpleType>
                  <restriction base = "string">
                    <enumeration value = "Observed"/>
                    <enumeration value = "Likely"/>
                    <enumeration value = "Possible"/>
                    <enumeration value = "Unlikely"/>
                    <enumeration value = "Unknown"/>
                  </restriction>
                </simpleType>
              </element>
              <element name = "audience" type = "string" minOccurs = "0"/>
              <element name = "eventCode" minOccurs = "0" maxOccurs =
"unbounded">
                <complexType>
                  <sequence>
                    <element ref = "cap:valueName"/>
```

```
                    <element ref = "cap:value"/>
                  </sequence>
                </complexType>
              </element>
              <element name = "effective" type = "dateTime" form = "qualified"
minOccurs = "0"/>
              <element name = "onset" type = "dateTime" minOccurs = "0"/>
              <element name = "expires" type = "dateTime" minOccurs = "0"/>
              <element name = "senderName" type = "string" minOccurs = "0"/>
              <element name = "headline" type = "string" minOccurs = "0"/>
              <element name = "description" type = "string" minOccurs = "0"/>
              <element name = "instruction" type = "string" minOccurs = "0"/>
              <element name = "web" type = "anyURI" minOccurs = "0"/>
              <element name = "contact" type = "string" minOccurs = "0"/>
              <element name = "parameter" minOccurs = "0" maxOccurs =
"unbounded">
                <complexType>
                  <sequence>
                    <element ref = "cap:valueName"/>
                    <element ref = "cap:value"/>
                  </sequence>
                </complexType>
              </element>
              <element name = "resource" minOccurs = "0" maxOccurs =
"unbounded">
                <complexType>
                  <sequence>
                    <element name = "resourceDesc" type = "string"/>
                    <element name = "mimeType" type = "string" minOccurs =
"0"/>
                    <element name = "size" type = "integer" minOccurs = "0"/>
                    <element name = "uri" type = "anyURI" minOccurs = "0"/>
                    <element name = "derefUri" type = "string" minOccurs =
"0"/>
                    <element name = "digest" type = "string" minOccurs = "0"/>
                  </sequence>
                </complexType>
              </element>
              <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                  <sequence>
                    <element name = "areaDesc" type = "string"/>
                    <element name = "polygon" type = "string" minOccurs = "0"
maxOccurs = "unbounded"/>
                    <element name = "circle" type = "string" minOccurs = "0"
maxOccurs = "unbounded"/>
                    <element name = "geocode" minOccurs = "0" maxOccurs =
"unbounded">
                      <complexType>
                        <sequence>
                          <element ref = "cap:valueName"/>
                          <element ref = "cap:value"/>
                        </sequence>
                      </complexType>
                    </element>
                    <element name = "altitude" type = "string" minOccurs =
"0"/>
                    <element name = "ceiling" type = "string" minOccurs = 0"/>
                  </sequence>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
      </sequence>
    </complexType>
  </element>
  <element name = "valueName" type = "string"/>
```

```
  <element name = "value" type = "string"/>
</schema>
```

8 Use of ASN.1 to specify and encode the CAP alert message

This clause provides the ASN.1 specification of the CAP alert message.

8.1 General

The ASN.1 specifciation (see ITU-T Rec X.680) in clause 8.3 provides an alternative formulation of the XML schema defined in clause 7.4. If the ASN.1 Extended XML Encoding Rules (see ITU-T Rec X.693) are applied to this ASN.1 schema, the permitted XML is identical to that supported by the XML schema in clause 7.4. If the ASN.1 Unaligned Packed Encoding Rules (see ITU-T Rec X.691) are applied to it, the resulting binary encodings are more compact than the corresponding XML encodings.

8.2 Formal mappings and specification

The normative specification of the compact binary encoding is in 8.3 with the application of the ASN.1 Unaligned Packed Encoding Rules (see ITU-T Rec. X.691).

The semantics of the fields in the ASN.1 specification are identical to those of the XSD specification, and the mapping of the fields from the XSD specification to the ASN.1 specification is formally defined in ITU-T Rec. X.694.

Implementations can produce and process the CAP alert XML messages using either ASN.1-based or XSD-based tools (or other ad hoc software).

Implementations can produce and process the CAP alert compact binary messages using ASN.1-based tools (or by other ad hoc software).

Any XML encoded CAP alert messages can be converted to compact binary messages by decoding with an ASN.1 tool configured for the Extended XML Encoding Rules and re-encoding the resulting abstract values with an ASN.1 tool configured for Unaligned Packed Encoding Rules.

Any compact binary CAP alert messages can be converted to XML encoded messages by decoding with an ASN.1 tool configured for Unaligned Packed Encoding Rules and re-encoding the resulting abstract values with an ASN.1 tool configured for Extended XML Encoding Rules.

8.3 ASN.1 Schema

```
CAP-1-1 {itu-t recommendation x cap(1303) version1-1(1)}
DEFINITIONS XER INSTRUCTIONS AUTOMATIC TAGS ::=
-- CAP Alert Message (version 1.1)
BEGIN

Alert ::= SEQUENCE {
   identifier IdentifierString,
       -- Unambiguous identification of the message
        -- from all messages from
       -- this sender, in a format defined by the sender and
        -- identified in the "sender" field below.
   sender     String,
       -- The globally unambiguous identification of the sender.
       -- This specification does not define the root of
        -- a global identification tree (there is no international
        -- agreement on such a root), so it relies
       -- on human-readable text to define globally and
```

```
       -- unambiguously the sender.
       -- An internet domain name or use of "iri:/ITU-T/..."
       -- are possible, but
       -- the choice needs to be clearly stated in human-readable form.
   sent        DateTime,
   status      AlertStatus,
   msgType     AlertMessageType,
   source      String OPTIONAL,
       -- Not standardised human-readable identification
      -- of the source of the alert.
   scope       AlertScope,
   restriction String OPTIONAL,
       -- Not standardised human-readable restrictions
       -- on the distribution of the alert message
   addresses   String OPTIONAL,
       -- A space separated list of addressees for private messages
       -- (see 7.2.1)
   code-list   SEQUENCE SIZE((0..MAX)) OF code String,
       -- A sequence codes for special handling
      -- (see 7.2.1)
       -- The format and semantics of the codes are not defined in this
       -- specification.
   note        String OPTIONAL,
       -- Not standardised human-readable clarifying text for the alert
       -- (see 7.2.1)
   references  String OPTIONAL,
       -- Space-separated references to earlier messages
     -- (see 7.2.1)
   incidents   String OPTIONAL,
       -- Space-separated references to related incidents
     -- (see 7.2.1)
   info-list   SEQUENCE SIZE((0..MAX)) OF info AlertInformation  }

AlertStatus ::= ENUMERATED {
        actual,
        draft,
        exercise,
        system,
        test }

AlertMessageType ::= ENUMERATED {
        ack,
        alert,
        cancel,
        error,
        update }

AlertScope ::= ENUMERATED {
        private,
        public,
        restricted }

AlertInformation ::= SEQUENCE {
   language          Language -- DEFAULT "en-US" -- ,
       -- The language used in this value of the Info type
     -- (see 7.2.2)
   category-list     SEQUENCE (SIZE(1..MAX)) OF
                     category InformationCategory,
   event             String,
       -- Not standardised human-readable text describing the
       -- type of the event (see 7.2.2)
   responseType-list SEQUENCE SIZE((0..MAX)) OF
                     responseType InformationResponseType,
   urgency           HowUrgent,
   severity          HowSevere,
   certainty         HowCertain,
   audience          String OPTIONAL,
       -- Not standardised human-readable text describing the
```

```
       -- intended audience for the message (see 7.2.2)
   eventCode-list    SEQUENCE SIZE((0..MAX)) OF eventCode SEQUENCE {
         valueName ValueName,
         value     Value },
   effective         DateTime OPTIONAL,
   onset             DateTime OPTIONAL,
   expires           DateTime OPTIONAL,
   senderName        String OPTIONAL,
      -- Not standardised human-readable name of the authority
       -- issuing the message (see 7.2.2)
   headline          String (SIZE (1..160,...)) OPTIONAL,
      -- Not standardised human-readable short statement (headline)
       -- of the alert (see 7.2.2)
   description       String OPTIONAL,
      -- Not standardised human-readable extended description of
       -- the event (see 7.2.2)
   instruction       String OPTIONAL,
      -- Not standardised human-readable recommended action
     -- (see 7.2.2)
   web               AnyURI OPTIONAL,
   contact           String OPTIONAL,
      -- Not standardised human-readable contact details for
       -- follow-up (see 7.2.2)
   parameter-list    SEQUENCE SIZE((0..MAX)) OF parameter SEQUENCE {
      -- System-specific parameters (see 7.2.2)
      valueName ValueName,
      value     Value },
   resource-list     SEQUENCE SIZE((0..MAX)) OF resource ResourceFile,
   area-list         SEQUENCE SIZE((0..MAX)) OF Area }

InformationCategory ::=  ENUMERATED {
        cBRNE,
        env,
        fire,
        geo,
        health,
        infra,
        met,
        other,
        rescue,
        safety,
        security,
        transport }

InformationResponseType ::= ENUMERATED {
        assess,
        evacuate,
        execute,
        monitor,
        none,
        prepare,
        shelter }

HowUrgent ::= ENUMERATED {
        expected,
        future,
        immediate,
        past,
        unknown }

HowSevere ::= ENUMERATED {
        extreme,
        minor,
        moderate,
        severe,
        unknown }

HowCertain ::= ENUMERATED {
```

```
        likely,
        observed,
        possible,
        unknown,
        unlikely }

ResourceFile ::= SEQUENCE {
       -- Information about an associated resource file
     -- (see 7.2.3)
   resourceDesc String,
       -- Not standardised human-readable description of the type
       -- and content of
       -- an associated resource file (for example a map or
       -- photograph)(see 7.2.3)
   mimeType     String OPTIONAL,
   size         INTEGER OPTIONAL, -- In bytes
   uri          AnyURI OPTIONAL,
   derefUri     String OPTIONAL,
       -- An alternative to the URI giving the Base64-encoded
       -- content of the resource file (see 7.2.3)
   digest       String OPTIONAL
       -- SHA-1 hash of the resource file for error detection
      -- (see 7.2.3) -- }

Area ::= SEQUENCE {
       -- Identification of an affected area
   areaDesc     String,
       -- Not standardised human-readable description of the area
   polygon-list SEQUENCE OF polygon String,
       -- Each element is a space-separated list of coordinate pairs
       -- The complete list starts and ends with the same point and
       -- defines the polygon that defines the area
     -- (see 7.2.4).
   circle-list  SEQUENCE OF circle String,
       -- A space-separated list of coordinates for a point and a radius
   geocode-list SEQUENCE SIZE((0..MAX)) OF geocode SEQUENCE {
       -- A geographic code designating the alert target area
     -- (see 7.2.4)
            valueName ValueName,
            value     Value },
   altitude     String OPTIONAL,
       -- Specific or minimum altitude of the affected area
   ceiling      String OPTIONAL
       -- Maximum altitude of the affected area -- }

ValueName ::=  String  -- A not standardised name for
       -- an information event code, a parameter or a geocode

Value ::=  String  -- The value of the information event code,
                   -- parameter or geocode

String ::=  UTF8String (FROM (
           {0,0,0,9} -- TAB
         | {0,0,0,10} -- CR
         | {0,0,0,13} -- LF
         | {0,0,0,32}..{0,0,215,255} -- Space to the start of the S-zone
         | {0,0,224,0}..{0,0,255,253} -- Rest of BMP after S-zone
         | {0,1,0,0}..{0,16,255,253}  -- Other planes -- ) )

StringChar ::= String (SIZE(1))

SpaceAndComma ::= UTF8String (FROM (
            {0,0,0,32} -- SPACE
          | {0,0,0,44} -- COMMA -- ) )

IdentifierString ::= String (FROM (StringChar EXCEPT SpaceAndComma))

Language ::= VisibleString(FROM ("a".."z" | "A".."Z" | "-" | "0".."9"))
```

```
                (PATTERN "[a-zA-Z]#(1,8)(-[a-zA-Z0-9]#(1,8))*")
      -- The semantics of Language is specified in IETF RFC 3066

DateTime ::= TIME (SETTINGS "Basic=Date-Time Date=YMD
          Year=Basic Time=HMS Local-or-UTC=LD")
       -- This is the ISO 8601 format using local time and a
       -- time difference

StringWithNoCRLFHT ::= UTF8String (FROM (
         {0,0,0,32}..{0,0,215,255}
         |{0,0,224,0}..{0,0,255,253}
         |{0,1,0,0}..{0,16,255,255}))

AnyURI ::= StringWithNoCRLFHT (CONSTRAINED BY {
          /* Shall be a valid URI as defined in IETF RFC 2396 */})

ENCODING-CONTROL XER
    GLOBAL-DEFAULTS MODIFIED-ENCODINGS
    GLOBAL-DEFAULTS CONTROL-NAMESPACE
        "http://www.w3.org/2001/XMLSchema-instance" PREFIX "xsi"
    NAMESPACE ALL, ALL IN ALL AS "urn:oasis:names:tc:emergency:cap:1.1"
              PREFIX "cap"
    NAME Alert, Area AS UNCAPITALIZED
    UNTAGGED SEQUENCE OF
    DEFAULT-FOR-EMPTY AlertInformation.language AS "en-US"
    TEXT AlertStatus:ALL,
         AlertMessageType:ALL,
         AlertScope:ALL,
         InformationCategory:ALL,
         InformationResponseType:ALL,
         HowUrgent:ALL,
         HowSevere:ALL,
         HowCertain:ALL AS CAPITALIZED
    WHITESPACE Language, AnyURI COLLAPSE
END
```

Appendix I

CAP Alert Message Examples

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

I.1 Homeland Security Advisory System Alert

The following is a speculative example in the form of a CAP XML message.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
<identifier>43b080713727</identifier>
<sender>hsas@dhs.gov</sender>
<sent>2003-04-02T14:39:01-05:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<scope>Public</scope>
   <info>
          <category>Security</category>
          <event>Homeland Security Advisory System Update</event>
          <urgency>Immediate</urgency>
```

```
         <severity>Severe</severity>
         <certainty>Likely</certainty>
         <senderName>U.S. Government, Department of Homeland
Security</senderName>
         <headline>Homeland Security Sets Code ORANGE</headline>
         <description>The Department of Homeland Security has elevated the
Homeland Security Advisory
         System threat level to ORANGE / High in response to intelligence
which may indicate a heightened
         threat of terrorism.</description>
         <instruction> A High Condition is declared when there is a high risk
of terrorist attacks. In
         addition to the Protective Measures taken in the previous Threat
Conditions, Federal departments
         and agencies should consider agency-specific Protective Measures in
accordance with their
         existing plans.</instruction>
         <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
                <parameter>
                       <valueName>HSAS</valueName>
                       <value>ORANGE</value>
                </parameter>
   <resource>
         <resourceDesc>Image file (GIF)</resourceDesc>
         <uri>http://www.dhs.gov/dhspublic/getAdvisoryImage</uri>
   </resource>
   <area>
         <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
   </area>
</info>
</alert>
```


I.2 Severe Thunderstorm Warning

The following is a speculative example in the form of a CAP XML message.


```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
<identifier>KSTO1055887203</identifier>
<sender>KSTO@NWS.NOAA.GOV</sender>
<sent>2003-06-17T14:57:00-07:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<scope>Public</scope>
<info>
   <category>Met</category>
   <event>SEVERE THUNDERSTORM</event>
   <responseType>Shelter</responseType>
   <urgency>Immediate</urgency>
   <severity>Severe</severity>
   <certainty>Observed</certainty>
   <eventCode>
         <valueName>same</valueName>
         <value>SVR</value>
   </eventCode>
   <expires>2003-06-17T16:00:00-07:00</expires>
   <senderName>NATIONAL WEATHER SERVICE SACRAMENTO CA</senderName>
   <headline>SEVERE THUNDERSTORM WARNING</headline>
<description> AT 254 PM PDT...NATIONAL WEATHER SERVICE DOPPLER RADAR INDICATED
A SEVERE THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY...OR ABOUT 18 MILES
SOUTHEAST OF KIRKWOOD...MOVING
SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND STRONG DAMAGING WINDS ARE LIKELY
WITH THIS STORM.</description>
```

```
   <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM
PASSES.</instruction>
   <contact>BARUFFALDI/JUSKIE</contact>
   <area>
   <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN CALIFORNIA, EXTREME
NORTHEASTERN CALAVERAS COUNTY IN CALIFORNIA, SOUTHWESTERN ALPINE COUNTY IN
CALIFORNIA</areaDesc>
   <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,-
120.14</polygon>
   <geocode>
          <valueName>FIPS6</valueName>
          <value>006109</value>
   </geocode>
   <geocode>
          <valueName>FIPS6</valueName>
          <value>006009</value>
   </geocode>
   <geocode>
          <valueName>FIPS6</valueName>
          <value>006003</value>
   </geocode>
   </area>
</info>
</alert>
```


I.3 Earthquake Report

The following is a speculative example in the form of a CAP XML message.


```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
<identifier>TRI13970876.1</identifier>
<sender>trinet@caltech.edu</sender>
<sent>2003-06-11T20:56:00-07:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<scope>Public</scope>
<incidents>13970876</incidents>
   <info>
          <category>Geo</category>
          <event>Earthquake</event>
          <urgency>Past</urgency>
          <severity>Minor</severity>
          <certainty>Observed</certainty>
          <senderName>Southern California Seismic Network (TriNet) operated by
Caltech and
          USGS</senderName>
          <headline>EQ 3.4 Imperial County CA - PRELIMINARY REPORT</headline>
          <description>A minor earthquake measuring 3.4 on the Richter scale
occurred near Brawley,
          California at 8:53 PM Pacific Daylight Time on Wednesday, June 11,
2003. (This is a computer-
          generated solution and has not yet been reviewed by a
human.)</description>
          <web>http://www.trinet.org/scsn/scsn.html</web>
          <parameter>
                        <valueName>EventID</valueName>
                        <value>13970876</value>
                 </parameter>
          <parameter>
                 <valueName>Version</valueName>
```

```
                <value>1</value>
          </parameter>
   <parameter>
          <valueName>Magnitude</valueName>
          <value>3.4 Ml</value>
   </parameter>
   <parameter>
          <valueName>Depth</valueName>
          <value>11.8 mi.</value>
   </parameter>
   <parameter>
          <valueName>Quality</valueName>
          <value>Excellent</value>
   </parameter>
   <area>
          <areaDesc>1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi.
E of OCOTILLO
          (quarry); 1 mi. N of the Imperial Fault</areaDesc>
          <circle>32.9525,-115.5527 0</circle>
   </area>
   </info>
</alert>
```


I.4 AMBER Alert (Including EAS Activation)

The following is a speculative example in the form of a CAP XML message.


```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
<identifier>KAR0-0306112239-SW</identifier>
<sender>KARO@CLETS.DOJ.CA.GOV</sender>
<sent>2003-06-11T22:39:00-07:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<source>SW</source>
<scope>Public</scope>
   <info>
          <category>Rescue</category>
          <event>Child Abduction</event>
          <urgency>Immediate</urgency>
          <severity>Severe</severity>
          <certainty>Likely</certainty>
          <eventCode>
                <valueName>SAME</valueName>
                <value>CAE</value>
          </eventCode>
   <senderName>LOS ANGELES POLICE DEPT - LAPD</senderName>
   <headline>AMBER ALERT</headline>
   <description>DATE/TIME: 06/11/03, 1915 HRS. VICTIM(S): KHAYRI DOE JR. M/B
BLK/BRO 3'0", 40
LBS. LIGHT COMPLEXION. DOB 06/24/01. WEARING RED SHORTS, WHITE T-SHIRT, W/BLUE
COLLAR. LOCATION: 5721 DOE ST., LOS ANGELES, CA. SUSPECT(S): KHAYRI DOE SR.
DOB 04/18/71 M/B, BLK HAIR,
   BRO EYE. VEHICLE: 81' BUICK 2-DR, BLUE (4XXX000).</description>
   <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-
2389</contact>
   <area>
   <areaDesc>Los Angeles County</areaDesc>
          <geocode>
                <valueName>SAME</valueName>
                <value>006037</value>
```

```
          </geocode>
   </area>
   </info>
</alert>
```

Bibliography

[b-WGS 84] National Geospatial Intelligence Agency, Department of Defense World Geodetic, System 1984, http://earth-info.nga.mil/GandG/publications/tr8350.2/tr8350_2.html, NGA Technical, Report TR8350.2, January 2000.

Multimedia Systems

ITU-T H.246 Amendment 1 (05/2006)

INTERWORKING OF H-SERIES MULTIMEDIA TERMINALS WITH H-SERIES MULTIMEDIA TERMINALS AND VOICE/VOICEBAND TERMINALS ON GSTN, ISDN AND PLMN: MAPPING OF USER PRIORITY LEVEL AND COUNTRY/INTERNATIONAL NETWORK OF CALL ORIGINATION BETWEEN H.225 AND ISUP

Summary

Amendment 1 amends Annex C/H.246 (ISDN User Part function – H.225.0 interworking) in support of mapping user priority level and country/international network of call origination between H.225 and ISUP.

Modifications introduced by this amendment are shown in revision marks. Unchanged text is replaced by ellipsis (…). Some parts of unchanged texts (clause numbers, etc.) may be kept to indicate the correct insertion points.

• • •

C.2 References

• • •

[1] ITU-T Recommendation Q.764 (1999), *Signalling System No. 7 – ISDN User Part signalling procedures, plus* Amendment 2 (2002), *Support for the International Emergency Preference Scheme*.

• • •

[21] ITU-T Recommendation H.460.4 (2002), Call priority designation for H.323 calls.

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

• • •

C.5.2 Parameters

• • •

Table C.2/H.246 – Mapping of ISUP parameters to H.225.0 information elements

ISUP parameter	H.225.0 information element
• • •	
Called party number	Called party number
Calling party's category	Call Priority Designation Parameter (ITU-T Rec. H.460.4)
Calling party number	Calling party number or sourceAddress

C.6.1.1.1 Mandatory parameters

•••

Calling party's category

Coded according to internal data of the interworking unit, except when the H.460.4 [21] Call Priority designation parameter is included in the SETUP message and it indicates a priority value of emergencyAuthorized. In this case, one of the following scenarios applies:

a) For an internal national gateway: If an internal national gateway receives a Call Priority designation parameter set to emergencyAuthorized, call establishment proceeds with priority. The CPC parameter in the outgoing IAM message should be set to the IEPS call marking value (0000 1110 [14]) or to a nationally assigned emergency call value. The actions taken on the ISUP side are described in 2.1.1.4 e/Q.764 [1] except that the ACM would be replaced by a Call Proceeding on the H.323 side.

b) For an outbound international gateway: If an outgoing international gateway receives a Call Priority designation parameter set to emergencyAuthorized, call establishment proceeds with priority. The CPC parameter in the outgoing IAM message should be set to the IEPS call marking value (0000 1110 [14]) or to a nationally assigned emergency call value. The actions taken on the ISUP side are described in 2.1.1.3 e/Q.764 [1] except that the ACM would be replaced by a Call Proceeding on the H.323 side.

c) For an inbound international gateway: If an inbound international gateway receives a Call Priority designation parameter set to emergencyAuthorized, and if there is a bilateral agreement between governmental authorities to support IEPS, then call establishment proceeds with priority. The CPC parameter in the outgoing IAM message should be set to the IEPS call marking value (0000 1110 [14]) or to a nationally assigned emergency call value. The actions taken on the ISUP side are described in 2.1.1.5 e/Q.764 [1] except that the ACM would be replaced by a Call Proceeding on the H.323 side.

d) For an intermediate international gateway: If an intermediate international exchange receives a Call Priority designation parameter set to emergencyAuthorized, call establishment proceeds with priority. The CPC parameter in the outgoing IAM message should be set to the IEPS call marking value (0000 1110 [14]) or to a nationally assigned emergency call value. The actions taken on the ISUP side are described in 2.1.1.4 e/Q.764 [1] except that the ACM would be replaced by a Call Proceeding on the H.323 side.

•••

C.6.1.1.2 Optional parameters

•••

MLPP precedence

NA.

C.6.1.2 Sending o f the Subsequent Address Message (SAM)

•••

C.7.1.1 Sending of the SETUP message

•••

Calling Party's Category

Coded according to the internal data of the interworking unit, except when the IAM contains a CPC value set to the IEPS call marking (0000 1110 [14]) or a nationally assigned emergency call value. In this case, the interworking function should include the Call Priority Designation parameter in the outgoing ARQ and SETUP messages. This parameter should be set to a priority value of emergencyAuthorized and the call establishment proceeds with priority. The priority extension coding is for future study. See ITU-T Rec. H.460.4 [21] for specific procedures.

Progress indicator

•••

ITU-T Rec. H.248.44 (01/2007)

GATEWAY CONTROL PROTOCOL: MULTI-LEVEL PRECEDENCE AND PRE-EMPTION PACKAGE

Summary

H.248.44 defines a package to provide signals and procedures necessary to realize multi-level precedence and pre-emption applications under H.248. While bandwidth and overload control, as well as judicious use of the Priority and Emergency ContextAttributes go a long way toward achieving these goals, existing systems also utilize tonal signals to inform end-users about the nature of the traffic, whether their current call is being pre-empted and whether or not their origination is being treated as priority traffic. These systems find a wide range of applications, including military command and control, government priority traffic and many disaster recovery and relief efforts. Priority traffic control and pre-emption are especially important in the time span immediately following a disaster when communications resources may be scarce.

1 Scope

This Recommendation defines a package that provides signals for use with precedence features, such as those used by military, government and disaster recovery applications. The support of this package is optional.

2 References

2.1 Normative references

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

– ITU-T Recommendation H.248.1 (09/2005), *Gateway control protocol: Version 3*.

2.2 Informative references

– ITU-T Recommendation H.460.14 (03/2004), *Support for Multi-Level Precedence and Preemption (MLPP) within H.323 systems*

– ITU-T Recommendation I.255.3 (07/1990), *Multi-level precedence and pre-emption service (MLPP)*

– ITU-T Recommendation Q.735.3 (03/1993), *Stage 3 description for community of interest supplementary services using Signalling System No. 7: Multi-level precedence and pre-emption*

– ETSI TS 124.067 (01/2005), *enhanced Multi-Level Precedence and Pre-emption service (eMLPP) – Stage 3*

– IETF RFC 4411 (02/2006), *Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events*

– IETF RFC 4412 (02/2006), *Communications Resource Priority for the Session Initiation Protocol (SIP)*

3 Definitions

3.1 Precedence: The assignment of a priority level to a call.

3.2 Pre-emption: The seizing of resources which are in use by a call of a lower precedence by a higher level precedence call in the absence of idle resources.

4 Abbreviations

This Recommendation uses the following abbreviations:

eMLPP Enhanced Multi-level Precedence and Pre-emption Service

IEPS International Emergency Priority Scheme

MG Media Gateway

MGC Media Gateway Controller

MLPP Multi-level Precedence and Pre-emption

5 Multi-level Precedence and Pre-emption Package

Package Name: Multi-level Precedence and Pre-emption Package

PackageID: prectn (0x009f)

Description: This package defines signals and procedures for use with precedence and pre-emption features, such as those used by military, government and disaster recovery applications.

Version: 1

Extends: None

5.1 Properties

None

5.2 Events

None

5.3 Signals

5.3.1 Preset Conference Notification Tone

Signal Name: Preset Conference Notification Tone

SignalID: preconf (0x0001)

Description: Generate preset conference notification tone, indicating that some conferees have not yet entered the conference. The physical characteristic of preset conference notification tone is available in the gateway.

Signal Type: Brief

Duration: Provisioned

Additional parameters: None

5.3.2 Preset Conference Precedence Notification Tone

Signal Name: Preset Conference Precedence Notification Tone

SignalID: pcprec (0x0002)

Description: Generate preset conference precedence notification tone, which is a provisionable alternative to the preset conference notification tone. The physical characteristic of preset conference precedence notification tone is available in the gateway.

Signal Type: Brief

Duration: Provisioned

Additional parameters: None

5.3.3 Precedence Ringing Tone

Signal Name: Precedence Ringing Tone

SignalID: precrt (0x0003)

Description: Generate precedence ringing tone, indicating that the call has importance above that of normal calls. The physical characteristic of precedence ringing tone is available in the gateway.

Signal Type: TimeOut

Duration: Provisioned

Additional parameters: None

5.3.4 Pre-emption Tone

Signal Name: Pre-emption Tone

SignalID: preempt (0x0004)

Description: Generate pre-emption tone, indicating that the call is being pre-empted for traffic of higher importance. The physical characteristic of pre-emption tone is available in the gateway.

Signal Type: Brief

Duration: Provisioned

Additional parameters: None

5.4 Statistics

None

5.5 Procedures

H.248.1 defines the Priority ContextAttribute as an integer taking a value 0-15, with 15 being the highest and 0 being the lowest priority. It also defines two ContextAttributes, Emergency and IEPS, which allow the MGC to mark a context as being used for the purposes of emergency or IEPS calls, respectively.

To date, there has been no formal definition of what a particular priority value means, or what the impact of the Emergency or IEPS ContextAttributes are on the priority value. H.248.11 makes use of priority to help in ameliorating overflow at the MG, but no indication as to what a particular priority value really means has been documented.

In the function of MLPP, particular calls are defined as being more important than other calls and are designated with named levels. These vary from network to network and from application to application. Table 1 provides several defined priority schemas. This does not imply any linkage between different schemas and is only provided as an informal survey of different priority schemas and their definitions. Please see the appropriate definition specifications to determine interaction requirements for a particular schema.

Table 1/H.248.44 – Existing priority schemas and algorithms

Priority	DSN/I.255.3	DRSN	Q.735.3	ETS	WPS	eMLPP
Highest ↓	Flash-Override	Flash-Override-Override[1]	0	0	0	A[2]
	Flash	Flash-Override	1	1	1	B[2]
	Immediate	Flash	2	2	2	0
	Priority	Immediate	3	3	3	1
	Routine	Priority	4	4	4	2
		Routine				3
Lowest						4
MLPP policy	Preemption	Preemption	Preemption	Priority Queuing	Priority Queuing	Both

NOTE 1 – Flash-Override-Override displaces existing calls, but once established becomes a Flash-Override call for the purposes of future preemptive calls.

NOTE 2 – A and B are only used on the local switch. For interswitch calls, A and B are treated as 0.

In addition to these, one has to consider the possibility that a provider has defined a "less-than-routine" call service level. This could be a lesser guaranteed level of service in exchange for reduced tariffs, for example. While not common in the PSTN today, it is possible in H.248 networks and has to be considered in the scope of the priority discussion overall.

In order to account for all these schemas, it is difficult to classify a particular schema as more or less important as another schema. Largely, these schemas operate on different networks (military or government networks, as opposed to the PSTN for example) and there is no need to identify how a particular schema aligns with another schema.

In terms of H.248, preemption is the act of forcibly removing terminations in order to free up facilities for another higher-precedence call. This allows the seizing of call/bearer resources which are in use by a call of a lower precedence by a higher level precedence call in the absence of idle resources.

Ultimately, the decision that a particular call is more important than another is the domain of the MGC. The Priority, IEPS and Emergency ContextAttributes are useful in allowing the MG to decide which calls to accept and which to reject in the case of overload control. Further, it allows the MG to perform dynamic resource allocation to ensure that a particular portion of its resources are available to handle higher priority calls that may come later. The priority designation and MLPP functionality are handled completely within the MGC, and any indication to the MG is secondary to the actual execution of the MLPP functions.

As indicated in the table, there are two common algorithms, namely, preemption and priority queuing. It is conceivable that both algorithms could be present in the same network. The algorithms are presented here for informational purposes:

Preemption

Schemas using a preemption policy may disrupt an existing call to make room for a higher-priority incoming call. Since calls may require different amounts of bandwidth or a different number of circuits, a single higher-priority call may displace more than one lower-priority call.

Priority Queuing

In a priority queuing policy, calls that find no available resources are queued to the queue assigned to the priority value. Unless otherwise specified, calls are queued in first-come, first-served order. Each priority value may have its own queue, or several priority values may share a single queue. If a resource becomes available, the MGC reattempts the call from the highest-priority non-empty queue according to the queue service policy. For first-come, first-served policies, the call from that queue that has been waiting the longest is served. Each queue can hold a finite number of pending calls. If the per-priority-value queue for newly arriving calls is full, the MGC may deny handling for the call immediately.

In addition, a priority queuing policy may impose a waiting time limit for each priority class, whereby setup times that exceed a specified waiting time are ejected from the queue and the call is deemed to have failed.

Finally, the MGC may impose a global queue size limit summed across all queues and drop waiting lower-priority calls attempts. This does not imply preemption, since the call was not previously established.

ITU-T Rec. H.460.4 (01/2007)

CALL PRIORITY DESIGNATION AND COUNTRY/INTERNATIONAL NETWORK OF CALL ORIGINATION IDENTIFICATION FOR H.323 PRIORITY CALLS

Summary

There is a desire to provide higher than normal priority call services to support several different applications. These applications include calls by authorized emergency personnel during disaster relief efforts, emergency calls by the public, or calls governed by service level agreements which specify a higher than normal probability of call completion. In order to provide these priority call services, it is necessary to signal to network elements such as Gatekeepers, Border Elements and Gateways that a call requires priority handling. This Recommendation defines messages and procedures necessary to signal the desired priority and country/international network of call origination for an H.323 priority call.

1 Scope

This Recommendation specifies the call priority designation and country/international network of call origination identification for H.323 priority calls. The use of the call priority designation provides a mechanism to indicate the desired or approved call establishment priority for an H.323 call. It is necessary to signal the call priority during registration, admission, location, and call setup signalling in order for the Gatekeepers, Gateways, and other network elements to take appropriate action to attempt to assure the successful establishment of priority calls over normal traffic during times of degraded operation due to damaged resources or heavy loads. The use of country/international network of call origination identifies the country or the international network of priority call origination. It is necessary to signal the country/international network of call origination during registration, admission, location, and call setup signalling in order for the Gatekeepers, Gateways, and other network elements to take appropriate action associated with the country or the international network of priority call origination.

The H.323 systems compliant with H.460.4 (11/02) are not required to generate or process the country/international network of call origination information.

2 References

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

[1] ITU-T Recommendation H.323 Version 4 (2000), *Packet-based multimedia communications systems*.

[2] ITU-T Recommendation H.225.0 Version 4 (2000), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[3] ITU-T Recommendation H.460.1 (2002), *Guidelines for the use of the generic extensible framework*.

[4] ITU-T Recommendation H.501 (2002), *Protocol for mobility management and intra/inter-domain communication in multimedia systems*.

[5] ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.

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

[7] ITU-T Recommendation H.246 (2006), *Interworking of H-series multimedia terminals with H-series multimedia terminals and voice/voiceband terminals on GSTN and ISDN*.

[8] Recommendation X.121 (1996), *International numbering plan for public data networks*.

[9] Recommendation E.164 (1997), *The international public telecommunication numbering plan*.

3 Terms and definitions

This Recommendation defines the following terms:

3.1 call priority: An indication of the importance of a call, as it relates to the probability of call completion and maintenance of call connection.

3.2 call completion: The ability to successfully make a call connection between a calling and called endpoint, assuming a called user is available to accept the call.

3.3 token: A piece of information, either clear or encrypted which can be used to validate a request for a specific call priority.

3.4 domain: A network or collection of networks under a single administrative authority that provides priority call establishment services.

3.5 country/international network of call origination: Information sent to identify the country or the international network of call origination.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ACF Admission Confirmation

ARQ Admission Request

ASN.1 Abstract Syntax Notation One

LCF Location Confirmation

LRQ Location Request

PDU Payload Data Unit

PIN Personal Identification Number

QoS Quality of Service

RAS Registration, Admission and Status

RCF Registration Confirmation

RRQ Registration Request

5 Call priority and country/international network of call origination parameter definitions

There are times when it is important to indicate the desired or required importance of a call. This may be due to service level agreements, emergency communications, or other system requirements. This importance, or call priority, is represented by a Call Priority Designation feature parameter that may be used to control those elements of the network that affect the probability of call completion and minimize call loss. This is not used to specify the quality of the media streams, but pertains only to the completion of the call establishment process. Under normal circumstances, on a well-designed, lightly loaded network, this parameter may have no apparent effect. However, in times of degraded operation, due to damaged resources or heavy loads, the parameter may allow for preferential treatment of certain call classes.

Call priority is indicated by a priorityValue and an optional priorityExtension, which are described below. References to priority in the following clauses refer to this combination of priorityValue and priorityExtension.

The country/international network of call origination can aid countries in establishing bilateral agreements with regard to the exchange of priority calls and the treatment of such calls. For example, the country/international network of call origination may have a multi level preference scheme and may make an agreement with the country of call destination for this multi level preference scheme to be mapped onto that of the country of destination. The country/international network of call origination can aid in allowing administrations in making decisions to admit a priority call or to allow mapping of priority level between countries. The country/international network of call origination is represented by a Country/International Network of Call Origination Identification feature parameter that may be used to identify the country or the international network of priority call origination.

Country/international network of call origination is indicated by a numbering plan indicator, country code, and identification code (if needed), which are described below.

The priorityValue indicates a class of service that has a specific relative probability of call completion. Higher priority calls shall have a higher probability of call completion. The following table shows the relative priority of the different values.

Value	Priority
emergencyAuthorized	0 – Highest
emergencyPublic	1
High	2
Normal	3 – Lowest

The Numbering plan indicator indicates the numbering plan used for the number. It is either according to ITU-T Recommendation X.121 or ITU-T Recommendation E.164. A specific country of call origination is identified by a X.121 country code (3 digits). An international network of call origination is identified by an E.164 country code for international networks (3 digits) and an identification code (1 to 4 digits).

If new values are added, their relative priority shall be indicated in this clause. A domain is free to support and act on only a subset of the call priorityValues, or to treat multiple, adjacent values the same. A device receiving a priorityValue that is not supported within its domain, may respond by assigning a Normal priority to the call. The action to be taken by any device in response to a specified call priority is outside the scope of this Recommendation and is subject to the local policy of the domain.

Any call that does not contain a Call Priority Designation feature parameter is assumed to be of Normal priority.

The priorityExtension may be used to indicate sub-priorities within a given priority class or may be used to indicated sub-classes of service within a given priority class. In the former case, it is recommended that higher extension values indicate higher priority levels. In the latter case, the values have no relative priority, but are used to indicate different sub-classes that may be handled differently. A domain is free to support and act on only a subset of the priorityExtension values, or to treat multiple values the same. A device receiving a priorityExtension value that is not supported within its domain, may respond by ignoring the priorityExtension or by treating it the same as any other value. The action to be taken by any device in response to a specified priorityExtension is outside the scope of this Recommendation and is subject to the local policy of the domain.

Call priority policy, value assignment and action are local matters confined to the scope of a domain. Mapping of call priority values and extensions, as well as coordination of actions between domains, is the subject of agreements between domains and is outside the scope of this Recommendation. It is recommended that priorityValues be mapped one-to-one and that they are preserved when passed through transit networks. However, there may be agreements specifying alternate mappings. For example, there may be circumstances under which HighPriority calls coming from another domain are mapped to Normal calls in the destination domain. The priorityExtension mappings need to be explicitly defined since the meaning of the priorityExtension is a local matter. This mapping may include removal of the priorityExtension.

The mapping of the Call Priority Designation and Country/International Network of Call Origination Identification between a packet network and a switched circuit network via a Gateway is described in ITU-T Rec. H.246.

Some priority levels may require authentication. A mechanism is provided to allow transmission of clear or encrypted tokens. These tokens may be used to validate the call priority request.

A call priority may be associated with an endpoint at registration time. This could provide a specific call priority for all calls made or received by the endpoint. A call priority may be associated with a call at admission and call setup time. This could provide a specific call priority on a per-call basis. The country/international network of call origination indication may also be associated likewise.

The calling endpoint may initiate the per-call call priority request, or a local or remote Gatekeeper may initiate it. The Gatekeeper may initiate a call priority request after detecting that the called endpoint requires a specific call priority. If a priority call is initiated, the country/international network of call origination shall be included.

The call priority and country/international network of call origination information is sent to allow Gatekeepers, Gateways, and other network elements to take specific action. The action to be taken is outside the scope of this Recommendation and would depend on service level agreements between the user and the provider, but may include:

– Priority admission confirmation;
– Priority access to gateways;
– Approval of bandwidth requests;
– Request for transport layer QOS from network elements;
– Authentication of service level request;
– Other actions to assure a specific probability of call completion.

The inability of a network, or network element, to provide the call priority requested in the Call Priority Designation feature shall not cause a call to fail. If a device cannot support, authorize, or understand a requested call priority, the action shall be to attempt to complete the call as a normal call or at another priority level that the domain supports.

It is important to note that in many cases, a priority call will be made from an endpoint that does not support the Call Priority Designation feature. In this case, the Gatekeeper or other network element must detect that the call requires a specific priority, and then signal that priority on behalf of the endpoint. For example, in emergency situations, emergency personnel may need to place a call from any endpoint. The capability of that endpoint cannot restrict the call priority. The emergency user could dial an access phone number and provide authentication, possibly via a PIN. The endpoint would then provide the follow-on dialling information. This access number would need to be detected by the Gatekeeper or other network element in order to mark the follow-on call with emergencyAuthorized priority. The mechanism for authenticating PIN numbers and accepting follow-on dialling information is outside the scope of this Recommendation, but it is expected that this could be provided by an interactive voice response system within the Gatekeeper, or some other feature server, which would be addressed by the access number. If the Gatekeeper initiates a priority call and includes the priority value, it shall also include the country/international international network of call origination.

In all instances when a priority call is created, the country/international network of call origination shall be included.

6 Messages and signalling

There are two call priority parameters defined in this Recommendation. They are:

– CallPriorityRequest;
– CallPriorityConfirm.

There are two country/international network of call origination parameters defined in this Recommendation. They are:

– Country/InternationalNetworkCallOriginationRequest;
– Country/InternationalNetworkCallOriginationConfirm.

The call priority parameter and country/international network of call origination parameter are transported in the H.225.0 RAS, H.225.0 Call Signalling (Q.931), Annex G/H.225.0, and H.501 messages using the generic extensibility framework as defined in ITU-T Rec. H.460.1, as follows:

– The CallPriorityRequest parameter may be sent in the call signalling SETUP message, and the CallPriorityConfirm parameter may be sent in the call Signalling CONNECT message. In these cases, the CallPriorityRequest or CallPriorityConfirm parameter is coded within the Call Priority Designation feature, which is placed in the genericData parameter in the H.225.0 H323-UU-PDU in the User-user Information Element.
– The Country/InternationalNetworkCallOriginationRequest parameter may be sent in the call signalling SETUP message. In this case, the CallPriorityRequest is coded within the Country/International Network of Call Origination feature, which is placed in the genericData parameter in the H.225.0 H323-UU-PDU in the User-user Information Element.
– The CallPriorityRequest parameter may be sent in the RAS channel RRQ, ARQ, or LRQ message, and the CallPriorityConfirm parameter may be sent in the RAS channel RCF, ACF, or LCF message. In these cases, the CallPriorityRequest or CallPriorityConfirm parameter is coded within the Call Priority Designation feature, which is placed in the genericData parameter in the request, or confirm (for example RegistrationRequest) parameter of the H.225.0 RasMessage element.

– The Country/InternationalNetworkCallOriginationRequest parameter may be sent in the RAS channel RRQ, ARQ, or LRQ message, and the Country/InternationalNetworkCall Origination Confirm parameter may be sent in the RAS channel RCF, ACF, or LCF message. In these cases, the Country/InternationalNetworkCallOriginationRequest or Country/InternationalNetwork Call OriginationConfirm parameter is coded within the Country/International Network of Call Origination feature, which is placed in the genericData parameter in the request, or confirm (for example RegistrationRequest) parameter of the H.225.0 RasMessage element.
– The CallPriorityRequest parameter may be sent in the Annex G/H.225.0 or H.501 Access Request message, and the CallPriorityConfirm parameter may be sent in the Annex G/H.225.0 or H.501 Access Confirmation message. In these cases, the CallPriorityRequest or CallPriorityConfirm parameter is coded within the Call Priority Designation feature, which is placed in the genericData parameter in the Annex G/H.225.0 AnnexGCommonInfo element or the H.501 Message CommonInfo element.
– The Country/InternationalNetworkCallOriginationRequest parameter may be sent in the Annex G/H.225.0 or H.501 Access Request message, and the Country/ International Network Call OriginationConfirm parameter may be sent in the Annex G/H.225.0 or H.501 Access Confirmation message. In these cases, the Country/InternationalNetworkCallOriginationRequest or Country/ InternationalNetworkCallOriginationConfirm parameter is coded within the Country/International Network of Call Origination feature, which is placed in the genericData parameter in the Annex G/H.225.0 AnnexGCommonInfo element or the H.501 MessageCommonInfo element.

The CallPriorityRequest or CallPriorityConfirm parameter contains the ASN.1 CallPriorityInfo structure, which contains the appropriate call priority fields. Similarly, the Country/ International Network Call OriginationRequest and Country/InternationalNetworkCallOriginationConfirm parameters are encoded using the ASN.1 Country/InternationalNetworkCallOriginationInfo structure and contains the appropriate country/international network of call origination fields.

7 Call priority procedures

7.1 Call priority and country/international network of call origination request during registration

An endpoint may wish to establish a specific call priority for all calls originating and/or terminating at that endpoint. This is useful in establishing a priority dial tone service, or indicating that the endpoint is a priority destination. To do this, the endpoint shall include the CallPriorityRequest in the RRQ message. This element specifies the desired priority for all calls originating and terminating at the endpoint.

If the Gatekeeper supports the Call Priority Designation feature, it shall reply with the CallPriorityConfirm in the RCF message. If the Gatekeeper is able to grant the requested priority, then the CallPriorityConfirm shall contain the same priority as the request. If the Gatekeeper is unable to grant the request, then the CallPriorityConfirm shall contain the priority that can be granted and the rejectReason value shall be set to priorityUnavailable.

If a CallPriorityConfirm is not returned, it shall be assumed that the Gatekeeper does not support the Call Priority Designation feature.

The endpoint may include a token in the CallPriorityRequest contained in the RRQ. This token may be used by the Gatekeeper to authenticate the call priority request. The mechanism for giving this token to the endpoint is outside the scope of this Recommendation. If a token is required by the Gatekeeper, and is either not present or not valid, the Gatekeeper may revert the call priority to Normal, and shall respond with the CallPriorityConfirm containing the new priority and the rejectReason value set to priorityUnauthorized.

The Gatekeeper may return a token in the CallPriorityConfirm contained in the RCF. This token may be used by the endpoint to indicate, in subsequent messages, that the Gatekeeper has authorized the request. If the token is present, the endpoint shall include it in all subsequent ARQ, SETUP, and CONNECT messages that originate at the endpoint.

Once a Gatekeeper returns a CallPriorityConfirm within the RCF, all calls to or from the registered endpoint shall be treated by the Gatekeeper as having the confirmed priority, regardless of the priority signalled in the ARQ (including no priority request), unless the endpoint indicates a higher priority for a specific call. The Gatekeeper shall follow the procedure described in 7.2, however, if the Gatekeeper cannot support the higher priority requested, it shall not confirm a priority lower than the one confirmed in the RCF.

When a priority call is created, the endpoint shall include the Country/International Network CallOriginationRequest in the RRQ message. This element identifies the country or international network of priority call origination and will contain the identity of the entity (the country or international network) originating the priority call.

If the Gatekeeper supports a priority call, it shall reply with the Country/ International Network CallOriginationConfirm in the RCF message.

7.2 Call priority and country/international network of call origination request during admission request

7.2.1 Request by endpoint

An endpoint may wish to establish a specific call priority for a call originating or terminating at that endpoint. To do this, the endpoint shall include the CallPriorityRequest in the ARQ message. This specifies the desired priority for this call.

If the Gatekeeper supports the Call Priority Designation feature, it shall reply with the CallPriorityConfirm in the ACF message. If the Gatekeeper is able to grant the requested priority, then the CallPriorityConfirm shall contain the same priority as the request. If the Gatekeeper is unable to grant the request, then the CallPriorityConfirm shall contain the priority that can be granted and the rejectReason value set to priorityUnavailable.

If a CallPriorityConfirm is not returned, it shall be assumed that the Gatekeeper does not support the Call Priority Designation feature.

The endpoint may include a token in the CallPriorityRequest contained in the ARQ. This token may be used by the Gatekeeper to authenticate the call priority request. This token may have been received by the endpoint in a previous RCF, or may have been received through some other mechanism that is outside the scope of this Recommendation. If a token is required by the Gatekeeper, and is either not present or not valid, the Gatekeeper may revert the call priority to Normal, and shall respond with the CallPriorityConfirm containing the new priority and the rejectReason value set to priorityUnauthorized.

The Gatekeeper may return a token in the CallPriorityConfirm contained in the ACF. This token may be used by the endpoint to indicate, in subsequent messages, that the Gatekeeper has authorized the request. If the token is present, the endpoint shall include it in the subsequent SETUP or CONNECT message sent by the endpoint for this call.

When a priority call is created, the endpoint shall include the Country/International Network CallOriginationRequest in the ARQ message. This element identifies the country or international network of priority call origination and will contain the identity of the entity (the country or international network) originating the priority call.

If the Gatekeeper supports a priority call, it shall reply with the Country/International Network CallOriginationConfirm in the ACF message.

7.2.2 Request by gatekeeper

If the endpoint does not include a CallPriorityRequest in the ARQ message, the Gatekeeper may wish to establish a specific call priority for a call originating or terminating at the endpoint. This may be useful for marking emergencyPublic priority for calls to emergency numbers such as 911, 119, or 999. To do this, the Gatekeeper shall include a CallPriorityConfirm in the ACF message. This element shall specify the priority that the Gatekeeper wants for the call.

If the endpoint supports the Call Priority Designation feature, it shall include the CallPriorityRequest containing the priority in the subsequent SETUP or CONNECT messages for this call.

If the endpoint does not support the Call Priority Designation feature, the CallPriorityConfirm shall be ignored. In this case, there is no mechanism for marking the call signalling messages unless the Gatekeeper is using the Gatekeeper Routed call signalling model, in which the Gatekeeper may modify the subsequent SETUP or CONNECT call signalling messages to include the CallPriorityRequest.

If the Gatekeeper establishes a specific priority call and includes the priority value, it shall include the Country/InternationalNetworkCallOriginationConfirm in the ACF message. This element identifies the country or international network of priority call origination and shall contain the identity of the entity (the country or international network) originating the priority call.

If the endpoint creates a priority call and includes the priority value, it shall include the Country/InternationalNetworkCallOriginationRequest containing the identity of the entity (the country or international network) originating the priority call in the subsequent SETUP message for this call.

7.3 Call priority and country/international network of call origination request during call setup

7.3.1 Request by calling endpoint

A calling endpoint may wish to establish a specific call priority for a call originated by that endpoint. To do this, the calling endpoint shall include the CallPriorityRequest in the SETUP message. This element shall specify the desired priority for this call. This is particularly useful if the called endpoint has resources that may be allocated based, on priority requests such as a Gateway or Multipoint Control Unit.

If the called endpoint supports the Call Priority Designation feature, it shall first forward that request to its Gatekeeper in the ARQ message. In this case, the procedures of 7.2.1 shall be followed.

After receiving the ACF from the Gatekeeper, the called endpoint shall reply with the CallPriorityConfirm in the CONNECT message. If the called endpoint is able to grant the priority returned by the Gatekeeper, then the CallPriorityConfirm in the CONNECT message shall contain the same priority as that received from the Gatekeeper. If the endpoint is unable to grant the request, then the CallPriorityConfirm shall contain the priority that can be granted and the rejectReason value set to priorityUnavailable.

If no CallPriorityConfirm is returned, it shall be assumed that either the called endpoint or its Gatekeeper do not support the Call Priority Designation feature.

The calling endpoint may include a token in the CallPriorityRequest contained in the SETUP message. This token may be used by the called endpoint to authenticate the call priority request. This token may have been received in a previous RCF, ACF, or may have been received through some other mechanism that is outside the scope of this Recommendation. If a token is required by the called endpoint, and is either not present or not valid, the called endpoint may revert the call priority to Normal, and shall respond with the CallPriorityConfirm containing the new priority and the rejectReason value set to priorityUnauthorized.

The called endpoint may return a token in the CallPriorityConfirm contained in the CONNECT message. This token may be used by the calling endpoint in subsequent calls to the called endpoint.

When a priority call is created, the endpoint shall include the Country/International Network CallOriginationRequest in the SETUP message. This element identifies the country or international network of priority call origination and will contain the identity of the entity (the country or international network) originating the priority call.

In case of endpoints that are connected to a home network through VPN, the call priority and country/international network of call origination information shall be inserted by the home network.

7.3.2 Request by called endpoint

If the calling endpoint does not include a CallPriorityRequest in the SETUP message, the called endpoint may wish to establish a specific call priority for the call.

If the called endpoint supports the Call Priority Designation feature, it shall first send the CallPriorityRequest to its Gatekeeper in the ARQ message. In this case, the procedures of 7.2.1 shall be followed.

After receiving the ACF from the Gatekeeper, the called endpoint shall forward the received CallPriorityConfirm in the CONNECT message.

If no CallPriorityConfirm is returned, it shall be assumed that the gatekeeper does not support the Call Priority Designation feature. In this case, the called endpoint may forward the original CallPriorityConfirm in the CONNECT message.

The called endpoint may return a token in the CallPriorityConfirm contained in the CONNECT message. This token may be used by the calling endpoint in subsequent calls to the called endpoint.

7.4 Call priority and country/international network of call origination request during location discovery

7.4.1 Request forwarded by calling endpoint's Gatekeeper

A Gatekeeper, which supports the Call Priority Designation feature, on receiving an ARQ containing the CallPriorityRequest for a called endpoint that is not in its zone, may forward the request to other Gatekeepers using the LRQ message. Alternatively, if the ARQ does not contain the CallPriorityRequest, but the Gatekeeper wishes to establish a call with a specific priority, the Gatekeeper may forward the CallPriorityRequest to other Gatekeepers in the LRQ message.

If the Gatekeeper receiving the LRQ containing the CallPriorityRequest recognizes the called endpoint as being in its zone and if the Gatekeeper supports the Call Priority Designation feature, it shall reply with the CallPriorityConfirm in the LCF message. If the Gatekeeper is able to grant the requested priority, then the CallPriorityConfirm shall contain the same priority as the request. If the Gatekeeper is unable to grant the request, then the CallPriorityConfirm shall contain the priority that can be granted and the rejectReason value set to priorityUnavailable.

If the CallPriorityConfirm is not returned, it is assumed that the Gatekeeper does not support the Call Priority Designation feature.

If a token is required by the called endpoint's Gatekeeper, and is either not present or not valid, the Gatekeeper may revert the call priority to Normal, and shall respond with the CallPriorityConfirm containing the new priority and the rejectReason value set to priorityUnauthorized.

The called endpoint's Gatekeeper may return a token in the CallPriorityConfirm contained in the LCF. This token may be used to indicate, in subsequent messages, that the Gatekeeper has authorized the request. If the token is present, the calling endpoint shall include it in the subsequent SETUP message sent by the endpoint for this call.

The calling endpoint's Gatekeeper, after receiving the LCF, shall in turn, forward the CallPriorityConfirm to the calling endpoint in the ACF. The calling endpoint's Gatekeeper may modify the CallPriority Confirm, or replace it if it cannot provide the indicated call priority.

If the Gatekeeper forwards a specific priority call request or wishes to establish a specific priority call, it may forward the Country/InternationalNetworkCallOriginationRequest to other Gatekeepers in the LRQ message.

If the receiving Gatekeeper supports a priority call, it shall reply with the Country/ International NetworkCallOriginationConfirm in the LCF message.

7.4.2 Request generated by called endpoint's Gatekeeper

A Gatekeeper, on receiving an LRQ that does not contain a CallPriorityRequest, may wish to establish a specific call priority for a call terminating at an endpoint in its zone. To do this, the Gatekeeper shall include the CallPriorityConfirm in the LCF message. This element specifies the desired priority that the Gatekeeper wants signalled for the call.

The calling endpoint's Gatekeeper, after receiving the LCF shall forward the CallPriorityConfirm to the calling endpoint in the ACF. If the calling endpoint's Gatekeeper is able to grant the requested priority, then the CallPriorityConfirm shall contain the same priority as the request. If the calling endpoint's Gatekeeper is unable to grant the request, then the CallPriorityConfirm shall contain the priority that can be granted and the rejectReason value set to priorityUnavailable.

If the calling endpoint's Gatekeeper does not support the Call Priority Designation feature, the CallPriorityConfirm shall be ignored.

An endpoint receiving an ACF containing the CallPriorityConfirm element shall follow the procedure in 7.2.2.

If the Gatekeeper establishes a specific priority call and includes the priority value, it shall include the Country/InternationalNetworkCallOriginationConfirm in the LCF message. This element identifies the country or international network of priority call origination.

The calling endpoint's Gatekeeper, after receiving the LCF, shall forward the Country/International NetworkCallOriginationConfirm to the calling endpoint in the ACF.

7.5 Call priority and country/international network of call origination indication during access request

7.5.1 Request forwarded by calling endpoint's gatekeeper/border element

A Gatekeeper/Border Element, which supports the Call Priority Designation feature, on receiving an ARQ containing the CallPriorityRequest for a called endpoint that is not in its zone, shall forward the request to other Border Elements in any Annex G/H.225.0 or H.501 AccessRequest message that it sends.

Alternatively, if the ARQ does not contain the CallPriorityRequest, but the Gatekeeper/Border Element wishes to establish a call with a specific priority, the Gatekeeper/Border Element may forward the CallPriorityRequest to other Gatekeepers in the AccessRequest message.

If the Border Element receiving the AccessRequest containing the CallPriorityRequest recognizes the called endpoint as being in its zone, and if the Border Element supports the Call Priority Designation feature, it shall reply with the CallPriorityConfirm in the AccessConfirmation message. If the Border Element is able to grant the requested priority, then the CallPriorityConfirm shall contain the same priority as the request. If the Border Element is unable to grant the request, then the CallPriorityConfirm shall contain the priority that can be granted, and the rejectReason value set to priorityUnavailable.

If the CallPriorityConfirm is not returned, it is assumed that the Border Element does not support the Call Priority Designation feature.

If a token is required by the Border Element, and is either not present or not valid, the Border Element may revert the call priority to Normal, and shall respond with the CallPriorityConfirm containing the new priority and the rejectReason value set to priorityUnauthorized.

The Border Element may return a token in the CallPriorityConfirm contained in the AccessConfirmation. This token may be used to indicate, in subsequent messages, that the Border Element has authorized the request. If the token is present, the calling endpoint shall include it in the subsequent SETUP message sent by the endpoint for this call.

The calling endpoint's Gatekeeper/Border Element, after receiving the AccessConfirmation, shall in turn, forward the CallPriorityConfirm to the calling endpoint in the ACF. The calling endpoint's Gatekeeper/Border Element may modify the CallPriorityConfirm or replace it if it cannot provide the indicated call priority.

In all instances when a priority call is created, the Country/InternationalNetworkCallOriginationRequest shall be included in the Annex G/H.225.0 or H.501 Access Request message, or Country/InternationalNetworkCallOriginationConfirm shall be included in the Annex G/H.225.0 or H.501 Access Confirmation message.

7.5.2 Request generated by responding Border Element

A Border Element, on receiving an AccessRequest that does not contain a CallPriorityRequest, may wish to establish a specific call priority for a call terminating at an endpoint in its zone. To do this, the Border Element shall include the CallPriorityConfirm in the AccessConfirmation message. This element specifies the desired priority that the Border Element wants signalled for the call.

The calling endpoint's Gatekeeper/Border Element, after receiving the AccessConfirmation, shall forward the CallPriorityConfirm to the calling endpoint in the ACF. If the calling endpoint's Gatekeeper/Border Element is able to grant the requested priority, then the CallPriorityConfirm shall contain the same priority as the request. If the calling endpoint's Gatekeeper/Border Element is unable to grant the request, then the CallPriorityConfirm shall contain the priority that can be granted and the rejectReason value set to priorityUnavailable.

If the calling endpoint's Gatekeeper does not support the Call Priority Designation feature, it shall ignore the CallPriorityConfirm.

An endpoint receiving an ACF containing the CallPriorityConfirm element shall follow the procedure in 7.2.2.

If the Border Element establishes a specific priority call and includes the priority value, it shall include the Country/InternationalNetworkCallOriginationConfirm in the AccessConfirmation message.

The calling endpoint's Gatekeeper/Border Element, after receiving the AccessConfirmation, shall forward the Country/InternationalNetworkCallOriginationConfirm to the calling endpoint in the ACF.

8 H.225.0 generic data usage

Generic extensibility framework shall be used to specify the call priority parameter and country/international network of call origination parameter for use in H.225.0 RAS and Call Signalling messages as described below.

8.1 Call Priority Designation feature and Country/International Network of Call Origination Identification feature tables

The following table defines the Call Priority Designation and Country/International Network of Call Origination Identification features.

Feature Name:	CallPriorityDesignation and Country/InternationalNetworkCallOriginationIdentification
Feature Description:	This data is sent in H.225.0 RAS, H.225.0 Call Signalling, Annex G/H.225.0, and H.501 messages to indicate the requested or approved priority for the call, or country/international network of call origination for the priority call.
Feature Identifier Type:	Standard
Feature Identifier Value:	4

8.2 Call Priority Designation parameter and Country/International Network of Call Origination Identification parameter tables

The following tables define the various parameters used to indicate call priority requests and confirmations. A Call Priority Designation GenericData message shall contain one, and only one, of the two defined parameters.

Parameter Name:	CallPriorityRequest
Parameter Description:	This is sent to indicate the requested priority for the call. The content is a raw field consisting of the ASN.1 PER encoded CallPriorityInfo as specified in the ASN.1 notation in Annex A.
Parameter Identifier Type:	Standard
Parameter Identifier Value:	1
Parameter Type:	Raw
Parameter Cardinality:	Once and Only Once

Parameter Name:	CallPriorityConfirm
Parameter Description:	This is sent to indicate the approved or allowed priority for the call. The content is a raw field consisting of the ASN.1 PER encoded CallPriorityInfo as specified in the ASN.1 notation in Annex A.
Parameter Identifier Type:	Standard
Parameter Identifier Value:	2
Parameter Type:	Raw
Parameter Cardinality:	Once and Only Once

The following tables define the various parameters used to indicate country/international network of call origination requests and confirmations. A Country/International Network of Call Origination Identification GenericData message shall contain one and only one of the two defined parameters.

Parameter Name:	Country/InternationalNetworkCallOriginationRequest
Parameter Description:	This is sent to indicate the country/international network of call origination for the priority call. The content is a raw field consisting of the ASN.1 PER encoded Country/InternationalNetworkCallOriginationInfo in the ASN.1 notation in Annex B.
Parameter Identifier Type:	Standard
Parameter Identifier Value:	3
Parameter Type:	Raw
Parameter Cardinality:	Once and Only Once

Parameter Name:	Country/InternationalNetworkCallOriginationConfirm
Parameter Description:	This is sent to indicate the country/international network of call origination for the priority call. The content is a raw field consisting of the ASN.1 PER encoded Country/InternationalNetworkCallOriginationInfo in the ASN.1 notation in Annex B.
Parameter Identifier Type:	Standard
Parameter Identifier Value:	4
Parameter Type:	Raw
Parameter Cardinality:	Once and Only Once

NOTE – Parameters 3 and 4 may not be present if the message is transmitted by the H.323 systems compliant with H.460.4 (11/02) that only utilize parameters 1 and 2.

Annex A/H.460.4

Call Priority and Country/International Network of Call Origination Identification ASN.1 definitions for use inside Generic Data

A.1 Call Priority and Country/International Network of Call Origination Identification ASN.1 definitions

```
CALL-PRIORITY {itu-t(0) recommendation(0) h(8) 460 4 version1(1)} DEFINITIONS
AUTOMATIC TAGS ::=
BEGIN

IMPORTS
         ClearToken,
         CryptoToken
     FROM H235-SECURITY-MESSAGES;

CallPriorityInfo  ::= SEQUENCE     -- root for Call Priority related asn.1
{
     priorityValue           CHOICE
     {
          emergencyAuthorized     NULL,
          emergencyPublic         NULL,
          high                         NULL,
          normal                            NULL,
          …
     },
     priorityExtension       INTEGER (0..255)   OPTIONAL,
     tokens                           SEQUENCE OF ClearToken OPTIONAL,
     cryptoTokens            SEQUENCE OF CryptoToken OPTIONAL,
     rejectReason            CHOICE
     {
          priorityUnavailable          NULL,
          priorityUnauthorized         NULL,
          priorityValueUnknown         NULL,
          …
     }    OPTIONAL,     -- Only used in CallPriorityConfirm
     …
}
CountryInternationalNetworkCallOriginationIdentification  ::= SEQUENCE
-- root for Country/International Network
-- of Call Origination Identification related asn.1
{
   numberingPlan CHOICE
   {
       x121 SEQUENCE
       {
           countryCode IA5String (SIZE (3)) (FROM ("0123456789")),
           ...
       },
       e164 SEQUENCE
       {
           countryCode IA5String (SIZE (3)) (FROM ("0123456789")),
           identificationCode IA5String (SIZE (1..4)) (FROM ("0123456789")),
           ...
       },
       ...
   },
   ...
}

END      -- of ASN.1
```

A.2 Description of New ASN.1 types and fields

CallPriorityInfo – Allows specification of call priority parameters within RAS and Call Signalling messages.

priorityValue – Identifies the priority of the call. This is used to indicate a specific probability of call completion. emergencyAuthorized is expected to be used for local, national, or other government emergency communications. emergencyPublic is to be used for public access to emergency services such as 911. High may be used for calls related to service level agreements that guarantee a specific probability of completion. Normal is used for calls that do not have a priority request.

priorityExtension – Allows subdivision or sub-grouping of the specified priority levels.

rejectReason – Used only in the Call Priority Confirm message to indicate why the requested priority is not provided. priorityUnavailable is used when the element cannot provide the requested priority. priorityUnauthorized is used when the element cannot authorize the requested priority. priorityUnknown is used when the element does not recognize the requested priority.

token, cryptoToken – These fields may contain tokens which indicate the authority to use or request specific Call Priorities.

CountryInternationalNetworkCallOriginationIdentification – Allows specification of country/ international network of call origination parameters within RAS and Call Signalling messages.

numberingPlan – Indicates the numbering plan used for the number.

x121 – Numbering plan according to ITU-T Recommendation X.121.

e164 – Numbering plan according to ITU-T Recommendation E.164.

countryCode – 3 digits code according to X.121 or E.164 to identify a specific country of call origination.

identificationCode – 1 to 4 digits code to identify an international network of call origination.

ITU-T Rec. H.460.14 (03/2004) – Prepublished version

SUPPORT FOR MULTI-LEVEL PRECEDENCE AND PREEMPTION (MLPP) WITHIN H.323 SYSTEMS

Summary

This Recommendation describes the procedures and the signalling protocol for Multi-Level Precedence and Preemption (MLPP), which allow the originator of a call in an H.323 environment to specify a precedence level of the call and for an existing lower precedence call to be preempted to release resources needed to complete that higher precedence call. For the networks and domains that allow this functionality, the H.460.14 mechanism ensures that important calls can be established and can remain connected during periods of congestion.

These procedures use the H.323 Generic Extensibility Framework (GEF) and therefore do not require any changes to the base standards.

1 Scope

Multi-Level Precedence and Preemption provides a framework for the treatment of calls based on precedence. It supports the preemption of active calls by higher-precedence calls when resources are limited. The system presented here is designed to be adaptable to different models of endpoints within H.323. It may be used to support direct endpoint call signalling or gatekeeper-routed endpoints of varying capabilities. For example, intelligent endpoints may support the MLPP procedures internally, while simple (e.g., stimulus-based) endpoints may require their Gatekeeper to implement the procedures in their stead. In the latter case, MLPP-specific signalling would be used only between Gatekeepers and other Gatekeepers or intelligent Gateways.

The elements of MLPP signalling are rather simple, hence they are defined using the tabular method described in ITU-T Rec. H.460.1.

2 Introduction

This Recommendation applies to H.323 endpoints (including Gateways) and Gatekeepers, and the interactions between them. It may be used with the direct endpoint call signalling model or the gatekeeper-routed model. This Recommendation provides signalling elements that may be used from one end of a call to the other, that is, from a calling endpoint, possibly through one or more Gatekeepers, to a destination endpoint.

In addition, two types of endpoints may be supported. Functional endpoints (e.g., those supporting H.450-series operations) are expected to support MLPP signalling to the endpoint, and should implement feature negotiation, user interaction, signalling, and timing in the endpoint. Stimulus-driven endpoints (e.g., those supporting Annex L/H.323) may remain ignorant of MLPP since the feature operation and interactions with the user are implemented within the controlling Gatekeeper or feature server. In either case, the elements of MLPP signalling defined herein should be used between Gatekeepers.

The following configurations are supported by the protocol defined in this Recommendation. It is possible for the various parties involved in an MLPP service to be using different configurations, that is, the following shall interwork.

2.1 Direct Endpoint Signalling

The configuration for the Direct Endpoint Signalling is as shown in Figure 1.

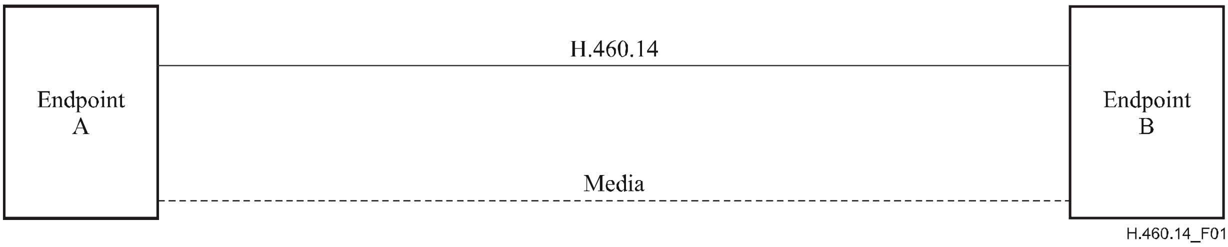


Figure 1/H.460.14 – Direct Endpoint Signalling configuration

This Recommendation describes the signalling required to support this configuration.

2.2 Gatekeeper Routed Signalling

Gatekeeper Routed Signalling has three cases as shown in Figure 2.

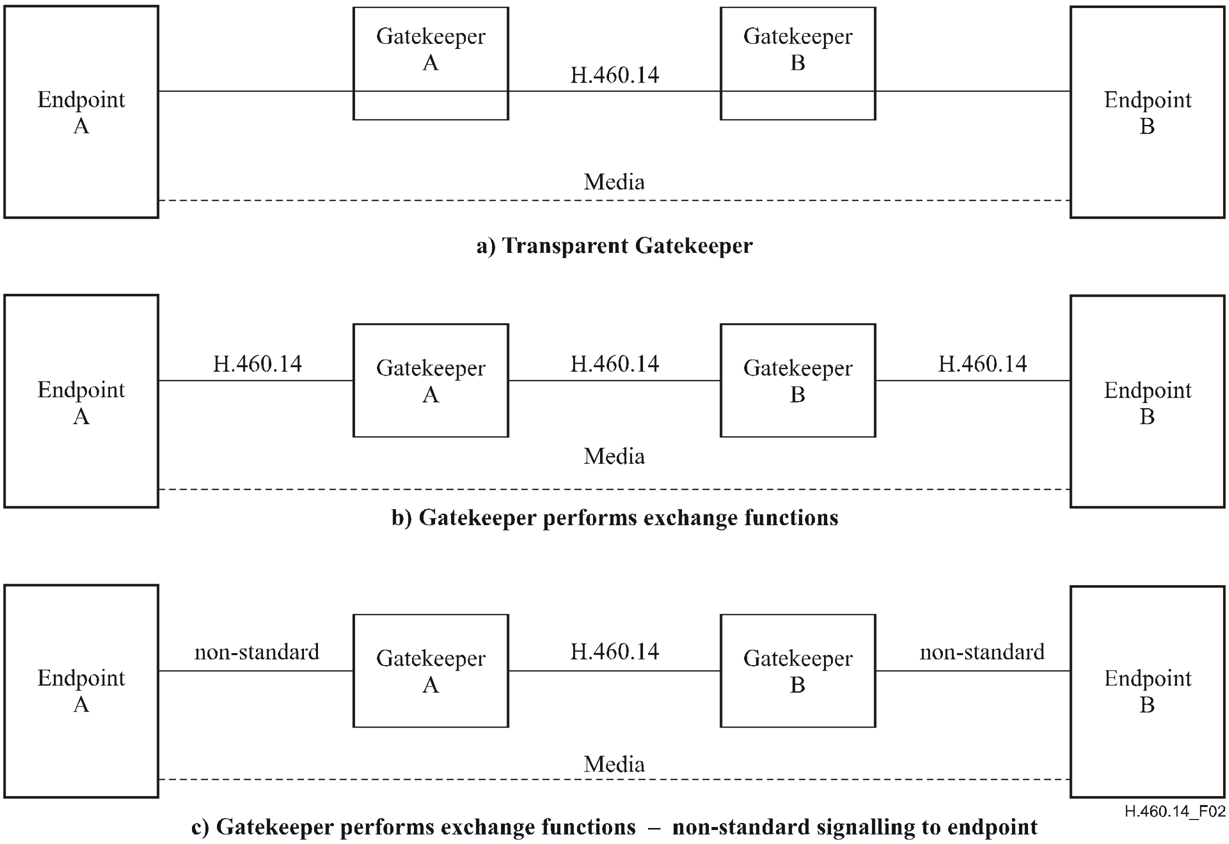


Figure 2/H.460.14 – Gatekeeper Routed Signalling configurations

For Configuration a, the Gatekeepers are completely transparent and only route the messages. The signalling between the endpoints is the same as for the Direct Endpoint Signalling case.

For Configuration b, the Gatekeepers terminate the call signalling messages and perform the exchange functions such as routing and feature interactions. The signalling between each Gatekeeper and its connected Endpoint and between the Gatekeepers is the same as for the Direct Endpoint Signalling case; however, the messages on each portion will be different.

For Configuration c, the Gatekeepers terminate the call signalling messages and perform the exchange functions such as routing and feature interactions. The signalling between the Gatekeepers is the same as for the Direct Endpoint Signalling case. This Recommendation does not address any non-standard protocol which might be used in Configuration c for communications with the endpoints.

2.3 Decomposed Gateway

As shown in Figure 19/H.323, an endpoint may be a gateway to the PSTN. It may be decomposed and utilize H.248 signalling as shown in Figure 3.

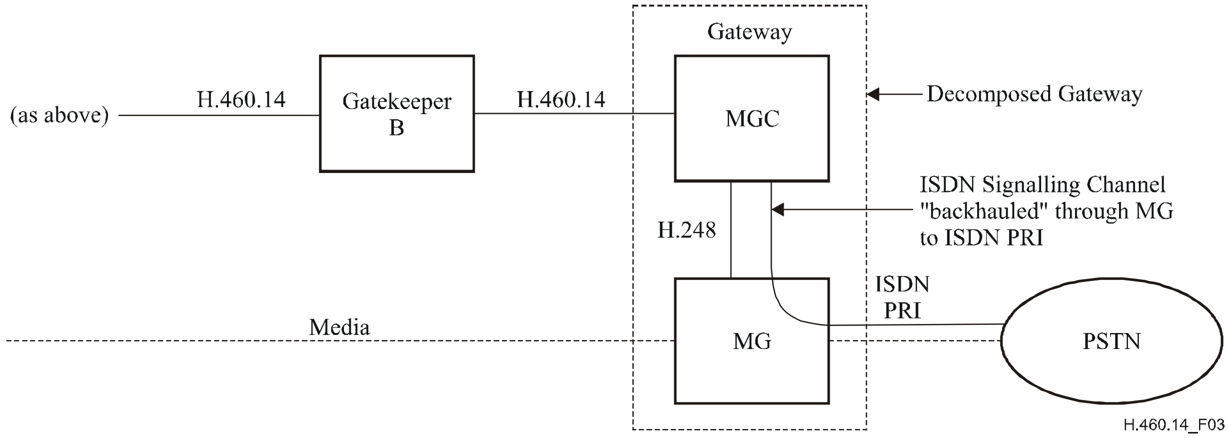


Figure 3/H.460.14 – Decomposed Gateway configuration

This Recommendation does not address the H.248 capabilities which may be required for this configuration.

2.4 H.248 managed devices

As shown in Figure 20/H.323, H.248 may be used to manage (control) the service operation in an endpoint. In this case, the end device functions as the Media Gateway portion of a decomposed Gateway as shown in Figure 4, but without capabilities related to interworking to other signalling systems.

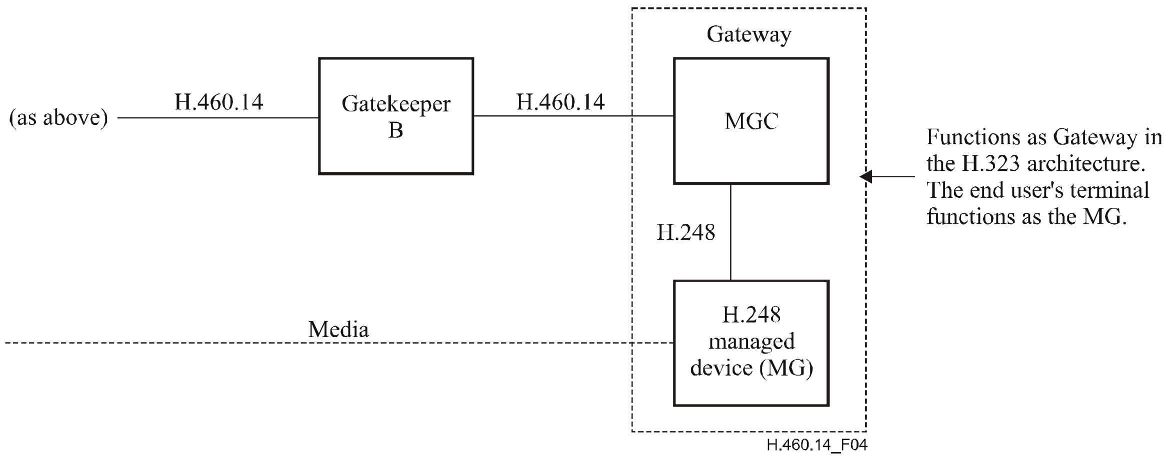


Figure 4/H.460.14 – H.248 managed device

This Recommendation does not address the H.248 capabilities which may be required for this configuration.

2.5 Stimulus device

An endpoint may operate using a stimulus protocol in accordance with Annex L/H.323 as shown in Figure 5 and Figure 21/H.323. The Feature Server functional entity may be associated with, or collocated with, a Gatekeeper.

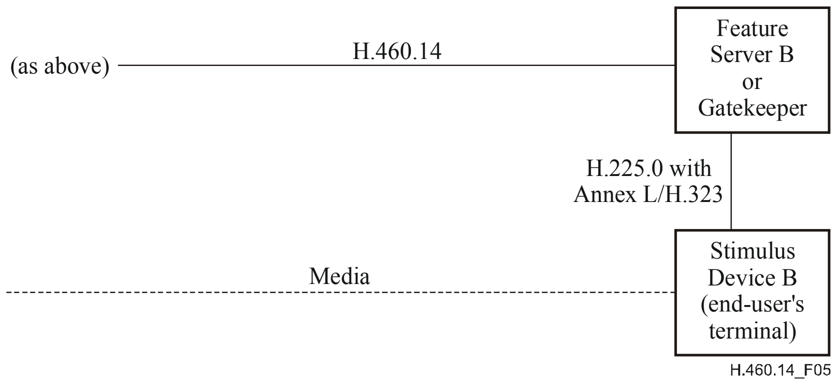


Figure 5/H.460.14 – Stimulus signalling using Annex L/H.323

This Recommendation does not address the signalling between the Feature Server/Gatekeeper and the Stimulus Device which may be required for this configuration. As described in ITU-T Rec. H.323 for interactions with H.450-services, the Feature Server must terminate the H.460 signalling and handle the MLPP operations described in this Recommendation, while using a stimulus protocol to signal via the terminal to the user as described in Annex L/H.323.

3 References

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

– ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

– ITU-T Recommendation H.245 (2003), *Control protocol for multimedia communication*.

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

– ITU-T Recommendations of the H.450.x series, *Supplementary services for multimedia*.

– ITU-T Recommendation H.460.1 (2002), *Guidelines for the Use of the Generic Extensible Framework.*

4 Definitions

This Recommendation defines the following terms:

4.1 alternate party: A third party to whom an MLPP call may be diverted if it is not accepted or acknowledged by the called user.

4.2 diversion: The operation in which a precedence call is redirected to a pre-assigned alternate party due to (in)action by the called party.

4.3 preemption: The act of forcibly removing a connection in order to free up facilities for another higher-precedence call.

4.4 preemption in progress: The period of time after a party is notified that their existing call is going to be preempted until the preemption actually occurs and is completed by the intended party acknowledging the action.

4.5 served user, user A: The user who requests to originate a call using MLPP (calling user).

4.6 user B: The wanted user that is subject to the call preemption (called user).

4.7 user C: The other user in the established call, also referred to as the unwanted user.

5 Abbreviations

This Recommendation uses the following abbreviations:

ACF Admission confirmation

ARJ Admission rejectation

ARQ Admission request

DCF Disengage confirmation

DRQ Disengage request

GCF	Gatekeeper confirmation
GK	Gatekeeper
GRQ	Gatekeeper request
LCF	Location confirmation
LRJ	Location rejectation
LRQ	Location request
MLPP	Multi-level precedence and preemption
RAS	Registration, admission and status
RCF	Registration confirmation
RRJ	Registration rejectation
RRQ	Registration request

6 Multi-level Precedence and Preemption Service description

The basic requirements for MLPP are the ability of call processing equipment to signal the precedence of each call, and for each entity (Gatekeeper, Gateway, or endpoint) which handles a call to properly manage resources for that call according to its precedence. This may well include the termination (preemption) of one or more active calls of lower precedence.

6.1 Provision of precedence levels

A maximum precedence level shall be allocated to each user, which shall have a value in the range from 4 (lowest level) to 0 (highest level). Each user shall be provided with a means to select a precedence for each call originated, not greater than the maximum allocated. If a precedence level is not explicitly selected for a call, the lowest value (4) shall be used. All five of the precedence level values shall be supported.

The Precedence levels are referred to as:

- 0 Flash Override
- 1 Flash
- 2 Immediate
- 3 Priority
- 4 Routine

The procedures by which the maximum precedence level is allocated to a user and the criteria by which a user chooses a value of precedence level for a particular call are outside the scope of this Recommendation.

6.2 Preemption of facilities

This Recommendation provides a means to identify the priority (precedence) of individual calls as they move through the network. It also defines signalling procedures for handling such calls when resource conflicts arise in the network or at an endpoint. When a facility (network bandwidth or endpoint hardware) is busy, and a call of higher precedence requires that facility, the facility may be preempted by termination of the existing call and establishment of the preempting call. If the facility is an endpoint under the control of a user, the user shall be notified of the presence of a preempting call, and must take action to accept the new call. When a call is preempted, special indication shall be given to all parties of that call to indicate that fact.

The decision to preempt a call is taken automatically by the call processing equipment and does not require any specific action of the called user. The details of how the existence of a precedence call or impending preemption is presented to the end user, or how the user indicates which actions to take, are beyond the scope of this Recommendation.

6.3 Diversion

A precedence call may be redirected (diverted) if an endpoint does not accept it within a specified time interval. The redirecting entity may indicate the new destination for the call.

6.4 Interactions with other services

Interactions with specific Supplementary Services defined in the H.450-series of Recommendations shall be as follows.

6.4.1 Call Transfer (CT)

User A shall not be able to invoke CT during the preemption in progress state on that call. (This is similar to the CT requirement that the call being transferred shall be answered before transfer can be initiated.) While performing CT, a user shall be allowed to invoke MLPP on the transfer request.

User B shall not be able to invoke CT during the preemption in progress state on the preempting call, that is, the call cannot be transferred until after the preemption is acknowledged and the new connection is established.

User C may be able to transfer an established call during preemption. In all cases, the transferred-to user that becomes connected to user B shall become the new user C, and shall receive all future notifications accordingly.

6.4.2 Call Forwarding Unconditional (CFU)

At User A: No service interaction.

At User B: If CFU is active when a call using MLPP arrives, CFU shall take precedence, i.e., the call shall be forwarded regardless of the precedence level of the call. If a call with a precedence level higher than the lowest is forwarded and is not responded to by any forwarded party, then the alternate party option of MLPP (using the alternate party of the original called party) shall apply.

However, if the network element controlling the call forwarding is aware that it is being used to forward to a voice mail system, it should apply the MLPP alternate party diversion instead of the Call Forwarding Unconditional.

At User C: No service interaction.

The precedence level of a call shall be preserved during the forwarding process. At the final diverted-to user (using CFB, CFU, or MLPP diversion), MLPP shall operate if that user is busy. However, if either CFNR or Call Deflection has taken place, the optional alternate party diversion shall not occur.

6.4.3 Call Forwarding Busy (CFB)

At User A: No interaction.

At User B: When a call using MLPP (with a precedence level greater than the lowest) arrives when User B is busy and has CFB active, the following order of preference shall apply:

- If the new call is of equal or lower precedence, or preemption is not possible for some other reason, CFB shall apply.
- If the new call is of higher precedence than an existing call, MLPP shall apply, i.e., preemption shall be used.
- If no answer is received for the CFB attempt, the alternate party option, if subscribed, shall apply. That is, the alternate party timer shall be used. If not subscribed, the normal failure procedures of CFB shall apply.

However, if the network element controlling the call forwarding is aware that it is being used to forward to a voice mail system, it should apply the MLPP alternate party diversion instead of the Call Forwarding Busy.

The precedence level of a call shall be preserved during the forwarding process. At the final diverted-to user (using CFB, CFU, or MLPP diversion), MLPP shall operate if that user is busy. However, if either CFNR or Call Deflection has taken place, the optional alternate party diversion shall not occur.

6.4.4 Call Forwarding on No Reply (CFNR)/Call Deflection (CD)

At User A: No interaction

At User B: When a call using MLPP (with a precedence level greater than the lowest) arrives and User B does not answer, the following shall apply:

- CFNR takes precedence over the Alternate Party.
- If the forwarded call is not responded to by any forwarded-to party within a specified period of time, the call shall then be diverted using the Alternate Party capability.

However, if the network element controlling the forwarding is aware that it is being used to forward to a voice mail system, it should apply the MLPP alternate party diversion instead of the Call Forwarding No Reply.

The precedence level of a call shall be preserved during the forwarding process. If either CFNR or Call Deflection has already taken place on the call, the optional alternate party diversion shall not occur.

6.4.5 Call Hold

At User A: There are no additional restrictions on Call Hold other than those defined for the CH service.

At User B: The preempting call shall not be put on hold. After it has been acknowledged and connected, it may be placed on hold. User B may put the established call to User C on hold as a means of becoming not busy.

6.4.6 Call Park

At User A: No service interaction.

At User B: It shall not be possible to park the preempting call until after it has been acknowledged and connected. User B may park the established call to User C as a means of becoming not busy.

6.4.7 Call Pickup

At User A: No service interaction.

At User B: MLPP shall take precedence over Call Pickup, i.e., if User B is busy, preemption shall occur rather than allowing others in the pickup group to retrieve the call. If User B is not busy, the call shall be placed in the pickup group and any member of that pickup group may answer it. If there is more that one call in the unanswered condition, a pickup attempt shall retrieve the one with the highest precedence level and, within a single level, the one which has been alerting the longest.

6.4.8 Call Waiting

At User A: No service interaction.

At User B: If a new call arrives for which MLPP is invoked and CW is subscribed, the interaction shall be as follows:

- If the new call is a higher precedence level than an existing call and preemption is possible, MLPP shall be used.
- If the new call is not a higher precedence level or User B is non-preemptable, CW shall be used.

6.4.9 Message Waiting Indication

No service interaction.

6.4.10 Name Identification

No service interaction.

6.4.11 Completion of Calls on Busy (CCBS)

At User A: It shall be possible to invoke MLPP with CCBS, that is, to specify a precedence level on a CCBS invocation.

At User B: If both MLPP invocation and CCBS are requested in the same call setup request, MLPP shall take precedence at User B, that is, an existing call will be preempted if possible. If not, the alternate party procedures shall be applied. If there is no alternate party specified, then CCBS shall apply. If the limit of number of calls waiting for CCBS has been reached, the new MLPP call may preempt an existing waiting call that is, take its place in the CCBS queue.

6.4.12 Completion of Calls on No Reply (CCNR)

At User A: It shall be possible to invoke MLPP with CCNR, that is, to specify a precedence level on a CCNR invocation.

At User B: If both MLPP and CCNR are requested in the same call setup request, MLPP shall take precedence at User B, that is, the alternate party procedures shall be applied. If there is no alternate party specified, then CCNR shall apply.

6.4.13 Call Offer (CO)

At User A: It shall be possible to request both CO and MLPP in the same call setup request.

At User B: If both MLPP invocation and CO invocation are requested at call set up, precedence shall be given to the MLPP service.

6.4.14 Call Intrusion

At User A: Call Intrusion and MLPP should not be requested in the same call setup request.

At User B: If a request for both Call Intrusion and MLPP is received in the same call setup request, the MLPP request shall take precedence.

6.4.15 Common information

At User A: By exchange of Common Information data, User A may have a priori knowledge of the MLPP capabilities at the called endpoint, e.g., the precedence level of existing calls at User B.

7 Signalling elements for MLPP

The following tables define the required signalling elements and parameters for MLPP utilizing the Generic Extensible Framework of H.323. The elements are defined in such a way that the MLPP capabilities may be easily extended by the definition of new parameters and no new ASN.1 definitions in ITU-T Rec. H.225.0 are required.

These parameters may be used in:

- H.501 Access Request and Service Request messages to perform inter-administrative domain address resolution and service negotiation.
- H.225.0 RAS messages to perform intra-domain address resolution and service negotiation.
- H.225.0 Call Signalling messages to control call setup.

7.1 Feature identifier

The feature identifier value in Table 1 is used to identify the feature in both the **featureSet** elements of H.225.0 and the **genericData** elements of H.225.0.

Table 1/H.460.14 – MLPP feature identifier

Feature name:	Multi-Level Precedence and Preemption (MLPP)
Feature description:	This feature provides the ability to associate a precedence level with each call, and to signal the preemption of facilities, based on relative call precedences.
Feature identifier type:	Standard
Feature identifier value:	14

The **featureSet** element provides the ability for an endpoint or Gatekeeper to indicate whether a feature is required (i.e., service cannot be provided without support for the feature), desired (i.e., the feature will be used if available), or supported (i.e., the feature will be used if the other party so desires) by that endpoint or Gatekeeper. An indication that a feature is required or desired implicitly indicates support. When used in the discovery/registration request/confirm messages (GRQ, GCF, RRQ, and RCF), the MLPP feature shall be specified as "required" or "desired". In all other messages, it shall be specified as "desired" or "supported". MLPP shall not be indicated as a "required" feature in ARQ, LRQ, or Setup because it is better to propagate the call without MLPP support than to have it blocked due to non-support.

The **genericData** is used to carry the MLPP parameters for a particular endpoint registration. It also provides the ability for an endpoint or Gatekeeper to indicate (in ARQ, LRQ, and Setup) that the MLPP feature is being used for a particular call. It implies support by the entity sending the message.

7.2 Parameter

This parameter is used to transport information between signalling entities within the MLPP **GenericData** element of requests and responses. In this Recommendation, "MLPP GenericData element" means a GenericData element which contains the MLPP feature identifier defined in Table 1.

Table 2/H.460.14 – MLPP information parameter

Parameter name:	MLPP Information
Parameter description:	This is the data sent in H.225.0 RAS and Call Signalling messages to indicate the use of MLPP. The contents is a raw field consisting of the ASN.1 encoded **MLPPInfo** as specified in Annex A. It shall be encoded in the basic aligned variant PER.
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	raw
Parameter cardinality:	Once and only once

The MLPP information definition used within the MLPP information parameter in the GenericData is shown in Annex A.

8 Procedures

The elements defined above may be employed in several ways to effect the desired call behaviours under MLPP when operating with the direct endpoint call signalling or the gatekeeper-routed model.

8.1 Registration, Admission and Status (RAS)

8.1.1 Gatekeeper discovery

When an endpoint attempts to find its Gatekeeper by sending a GatekeeperRequest (GRQ), it may include the **featureSet** element to indicate that it requires or desires support for MLPP. Each Gatekeeper that supports MLPP should respond with a Gatekeeper Confirm (GCF) containing a **featureSet** element which indicates support for MLPP. If the endpoint has not indicated support for MLPP, but the Gatekeeper requires it, the Gatekeeper may reply with GCF, but should indicate the requirement therein. If a Gatekeeper indicates that MLPP is required and the endpoint cannot support it, the endpoint should not attempt to register to that Gatekeeper.

8.1.2 Registration

When the endpoint registers (sends RRQ), it may include the **featureSet** element to indicate its support for MLPP. The Gatekeeper may respond with RCF if it can provide compatible support, but it shall reject the registration (with an RRJ) if it (the Gatekeeper) requires MLPP support by the endpoint and the endpoint does not indicate support.

8.1.3 Call Admission Control (CAC)

H.323 supports two types of call admission: ARQ/ACF/ARJ for endpoint-to-Gatekeeper signalling, and LRQ/LCF/LRJ for inter-Gatekeeper signalling. Both sequences are defined as part of RAS, not as part of call signalling, and are quite similar. If a Gatekeeper is to monitor consumption of resources, the use of RAS is necessary in the direct endpoint call-signalling model. It is also useful in the Gatekeeper-routed model, especially between Gatekeepers. Even though any Gatekeeper in the route could simply refuse the

Setup request, it is more efficient to reject an ARQ or LRQ. The CAC mechanisms may be illustrated with an MLPP call from endpoint A on Gatekeeper A to endpoint B on Gatekeeper B using the direct endpoint call-signalling model. This assumes all parties support MLPP.

In addition, the Access Request procedures defined in Annex G/H.225.0 may be used for inter-administrative domain address resolution. The parameters defined in this Recommendation may be included in the H.501 Messages.

Admission may be pre-granted at the time of registration.

A Direct Endpoint Call Signalling example

The first may be illustrated with an MLPP call from endpoint A on Gatekeeper A to endpoint B on Gatekeeper B using the direct endpoint call signalling model.

1) Endpoint A sends ARQ to Gatekeeper A, indicating endpoint B in the **destinationInfo** element and including an MLPP **genericData** element containing **precedence** with the desired value (2 for Immediate in this example).

2) Gatekeeper A examines the ARQ, and, if the request is allowed, replies with an ACF message. Gatekeeper A replies to endpoint A with ARJ if no facilities are available for calls of the requested precedence of 2. In that case, the ARJ contains an MLPP **genericData** element containing **mlppReason** with value 46 (callBlocked). The basis for this decision is beyond the scope of this Recommendation.

3) Endpoint A then establishes a call signalling channel to the address specified in the ACF (endpoint B's address in the direct endpoint call signalling model) and sends a Setup message to endpoint B as described in 8.2.1 containing an MLPP **genericData** element and **precedence** with value 2.

4) If endpoint B supports MLPP and is unable to accept the call (e.g., if it is busy with a higher precedence call), it applies the alternate party procedures if possible. Otherwise, it refuses the call by sending a Release Complete message containing a **reason** of **genericDataReason**, along with an MLPP **genericData** element with **mlppReason** with value 46 (CallBlocked) as described in 8.2.2.2.

   If endpoint B does not support MLPP and is unable to accept the call (e.g., it is busy), then it refuses the call by sending a Release Complete containing a **reason**, e.g., unreachable destination, without the MLPP **genericData** element.

5) If endpoint B is able to accept the offer of the call, it sends an ARQ to Gatekeeper B to gain permission. The ARQ contains an MLPP **genericData** element with **precedence** with the desired value (2 in this example).

6) If Gatekeeper B wishes to disallow the call due to precedence restriction, it returns an ARJ with an MLPP **genericData** element containing **mlppReason** with value 46 (call Bocked). The ARJ may contain an alternateParty structure. Endpoint B then sends a Release Complete back to endpoint A containing an MLPP **genericData** element with **mlppReason** with value 46 (callBlocked) and **alternateParty** as described in 8.2.2.2. If the call is rejected for some other reason, that reason is indicated by Gatekeeper B in **admissionRejectReason** and mapped back to the **release CompleteReason** returned to endpoint A, as appropriate.

7) If Gatekeeper B wishes to permit the call, it returns an ACF to endpoint B. If Gatekeeper B is able to identify a call that should be preempted, as might be the case if endpoint B is a trunk Gateway, this ACF contains an MLPP **genericData** element with a **releaseCall** structure which contains B, **releaseReason** set to 9 (preemption – facility reserved), and optionally **releaseDelay**. The Gatekeeper may also include the **alternateParty** structure if an alternate party is designated for endpoint B.

8) At this point, endpoint B is able to accept the call from endpoint A. If endpoint B is busy with another call that needs to be preempted, it carries out the release procedures prior to accepting the call from endpoint A by sending a Release Complete as described in 8.2.2.1. The first response it sends to endpoint A contains a **featureSet** which indicates whether or not endpoint B supports MLPP.

B Gatekeeper-routed example

If the above call were to be Gatekeeper-routed, then the following sequence would be used (assuming that discovery and registration were already done and admission was pre-granted during registration so that ARQ/ACF sequences are not used.)

1) Endpoint A sends a Setup to its Gatekeeper A, containing an MLPP **genericData** element containing **precedence** with the desired value (2 for Immediate, for example).

2) If Gatekeeper A cannot support the call at the indicated precedence, it returns a Release Complete with **reason** set to **genericDataReason**, along with an MLPP **genericData** element with **mlppReason** with value 46 (callBlocked).

3) If Gatekeeper A is able to support the call, it routes the call toward the destination via facilities that can admit a call of the indicated precedence (e.g., the precedence may be used to favour facilities that can support precedence over others that do not).

   If Gatekeeper A does not know which Gatekeeper will perform the function of Gatekeeper B for this call, it sends an LRQ message via multicast. If Gatekeeper A already knows the identity of the desired Gatekeeper B but not its signalling address, Gatekeeper A sends an LRQ message to Gatekeeper B on its RAS Channel TSAP Identifier. If Gatekeeper A already knows the identity and call signalling address of Gatekeeper B, it may send the Setup to it without first using the LRQ sequence.

   In any of the above three cases, the LRQ or Setup message contains an MLPP **genericData** element containing **precedence** with the desired value (2 for Immediate in this example).

4) When Gatekeeper B receives the LRQ, it determines whether or not it is able to admit a call based on the indicated precedence, and responds back to Gatekeeper A with an LCF if it is able, as defined in 7.2.3/H.323. If Gatekeeper B cannot support the call, it returns an LRJ message with an MLPP **genericData** element containing **mlppReason** with value 46 (callBlocked) or the appropriate **locationRejectReason** (e.g., **invalidPermission**).

   When Gatekeeper A receives the LRJ, it may attempt to route the call in a different manner, e.g., via a different Gatekeeper. If not, it returns a Release Complete to endpoint A with **reason** set to **genericDataReason**, along with an MLPP **genericData** element with **mlppReason** with value 46 (callBlocked).

5) When Gatekeeper A receives the LCF (with a call signalling address for Gatekeeper B and **featureSet** indicating support for MLPP), it sends a Setup message to that address containing an MLPP **genericData** element containing **precedence** with a value 2 (in this example) as described in 8.2.1.

6) When Gatekeeper B receives the Setup for the call, its actions depend on whether or not the intended endpoint B supports MLPP, which the Gatekeeper determined during registration.

   If endpoint B supports MLPP, Gatekeeper B sends a Setup to endpoint B and endpoint B performs the functions as described in 8.2.2. The Setup may contain the **releaseCall** structure if there is a call for endpoint B to preempt first and it may contain the **alternateParty** structure if an alternate party is assigned in case user B does not accept the precedence call.

   If endpoint B does not support MLPP, Gatekeeper B first performs any required preemption by sending a Release Complete on the call to be preempted, then sends a Setup, and provides timing for the alternate party as described in 8.2.2.

8.1.4 Call establishment and preemption

If a Gatekeeper receives a request to establish an MLPP call of a certain precedence, it may be necessary to terminate another call of lower precedence. This may be done by either a Gatekeeper or an endpoint. When terminating a call via a Release Complete, the terminating endpoint or Gatekeeper shall set the **reason** to **genericDataReason** and shall include an MLPP **genericData** element with **mlppReason** set to either 8 (to release all facilities) or 9 (to maintain facility reservations).

8.2 Call signalling procedures for H.450 endpoints

The procedures described in this clause apply to an endpoint using functional signalling, which is intended for endpoints which provide other Supplementary Services in accordance with the H.450-series of Recommendations.

These procedures require that the signalling channel for each call be maintained throughout the duration of the call. They also presume that the appropriate RAS procedures (discovery, registration and admission) are performed in the same way as for normal calls, with the addition of the indication of support for MLPP and the precedence level in the RAS messages. RAS actions are not included in this description, but are described in 8.1 and in ITU-T Rec. H.323.

While the text of this clause is written assuming the direct endpoint call signalling case, the actions stated for the endpoints may instead be performed by their Gatekeepers in the Gatekeeper-routed case. Further, the same signalling may be used between Gatekeepers and endpoints.

8.2.1 Actions at user A's endpoint

8.2.1.1 Normal procedure

To invoke MLPP for a new call, endpoint A shall perform the following actions (after any required RAS signalling as described in 8.1):

- Send a Setup message containing an MLPP **genericData** element with **precedence**, and enter state MLPP-Wait-Ack. The **precedence** shall convey the precedence level requested by the calling user.

In state MLPP-Wait-Ack, on receipt of a Connect message, endpoint A shall enter state MLPP-Idle. Establishment of media channels shall follow normal H.323 procedures. Normal call timers shall apply.

8.2.1.2 Exceptional procedure

In state MLPP-Wait-Ack, on receipt of a Release Complete message with or without any MLPP specific error, the MLPP call setup has failed and endpoint A shall enter state MLPP-Idle.

Failure of MLPP should be indicated to the calling user and the call shall continue in accordance with basic call procedures.

8.2.1.3 Procedure for completion of MLPP

In state MLPP-Wait-Ack, on receipt of Connect, either with or without an MLPP **genericData** element, the state MLPP-Idle shall be entered. If a **genericData** element contains **mlppNotification** with value **preemptionComplete**, the user at endpoint A shall be provided an indication of this.

8.2.1.4 Optional procedures for invocation of MLPP

In state MLPP-Wait-Ack, multiple Alerting messages may be received in the case of alternate party diversion at user B's endpoint. No further actions are required at user A's endpoint.

8.2.2 Actions at user B's endpoint

8.2.2.1 Normal procedure

If, while processing an incoming Setup message containing an MLPP **genericData** element with **precedence**, the called user is found to be busy, endpoint B shall check whether the called user is involved in a compatible active call (in the following, referred to as the "established call"), that the precedence level of that call is lower than the precedence level of the received call, and that there are no other reasons for denying preemption (e.g., if the established call is already being preempted or a requested option cannot be supported).

NOTE – The method by which endpoint B checks whether an active call is compatible with the new precedence call is outside the scope of this Recommendation.

If all conditions are met, endpoint B shall provide a notification of an impending preemption to the involved users. Endpoint B shall send on the established call (in a Facility message) and optionally also on the preempting call (in an Alerting message if possible, otherwise in a Progress or Facility message) an MLPP **genericData** element with **mlppNotification** set to value **preemptionPending**, shall start timer T6, and shall enter state MLPP-Dest-Notify. If endpoint B also provides a preemption warning tone, a Progress indicator information element with progress descriptor #8, *In-band information or an appropriate pattern is now available,* should be included in the Alerting or Progress message. If endpoint B does not provide tones, a Facility message should only be used. Execution of preemption shall commence on expiry of timer T6 in state MLPP-Dest-Notify.

8.2.2.2 Exceptional procedure

On receipt of a Setup message containing an MLPP **genericData** element with **precedence**, if the called user is not busy, the call shall continue according to basic call procedures, that is, endpoint B shall return normal Call Proceeding, Alerting, or Connect messages not containing any MLPP **genericData** element and shall remain in state MLPP-Idle.

If the called user is busy but invocation of MLPP is not possible (including the case where the precedence level of all calls at user B is too high), the preempting call shall be released. Endpoint B shall include an MLPP **genericData** element with **mlppReason** containing value 46 (callBlocked) in the Release Complete message and shall remain in state MLPP-Idle.

If, in the case of a normal preemption request during state MLPP-Dest-Notify, the called user becomes not busy and presentation of the preempting call becomes possible, normal call processing messages shall be returned to endpoint A, that is, Alerting, Connect, or Facility message, timer T6 shall be stopped, and state MLPP-Idle shall be entered.

Upon expiry of timer T6, endpoint B shall send a Release Complete message to endpoint C containing a **reason** of **genericDataReason** and an MLPP **genericData** element with **mlppReason** set to 8 (preemptionNoReservation). If an ARQ had been sent when this call was originally set up, endpoint B shall also send a DRQ to the Gatekeeper containing a **disengageReason** of **forcedDrop**, a **terminationReason** containing a **releaseCompleteReason** of **GenericDataReason**, and an MLPP **genericData** element with **mlppReason** containing value 9 (preemptionReservation).

8.2.2.3 Procedures for completion of MLPP

If the preempting call is released in any state, endpoint B shall enter state MLPP-Idle and stop any MLPP timer. If release occurs during state MLPP-Dest-Notify, the established call shall be restored to the state that existed prior to preemption and a Facility message containing an MLPP **genericData** element with **mlppNotification** set to value **preemptionEnd** shall be sent on the established call.

8.2.3 Actions at user C's endpoint

On receipt of a Facility message on an existing call containing an MLPP **genericData** element with **mlppReason** set to value 8 or 9, endpoint C may indicate the preemption status information to user C. It takes no other action.

On receipt of a Release Complete message, endpoint C releases the call with normal notification to the user. If the Release Complete contains the MLPP **genericData** element with **mlppReason** set to 8, endpoint C should notify the user of this.

9 Dynamic description

This clause provides a dynamic description of the operation of MLPP corresponding to the procedures described in 8.2 for the functional signalling case. It describes two cases:

– Direct endpoint call signalling model with endpoints directly exchanging functional signalling (without intervention by a Gatekeeper);

– Gatekeeper-routed model, with Gatekeepers exchanging functional signalling and performing service operations and signalling to endpoints via non-standardized (maybe stimulus) signalling.

The case of fully functional signalling between Gatekeepers as well as from Gatekeepers to endpoints is thereby possible using the procedures shown for the above two cases.

9.1 Operational model

Figure 6 shows the functional model for successful MLPP before and after MLPP invocation.

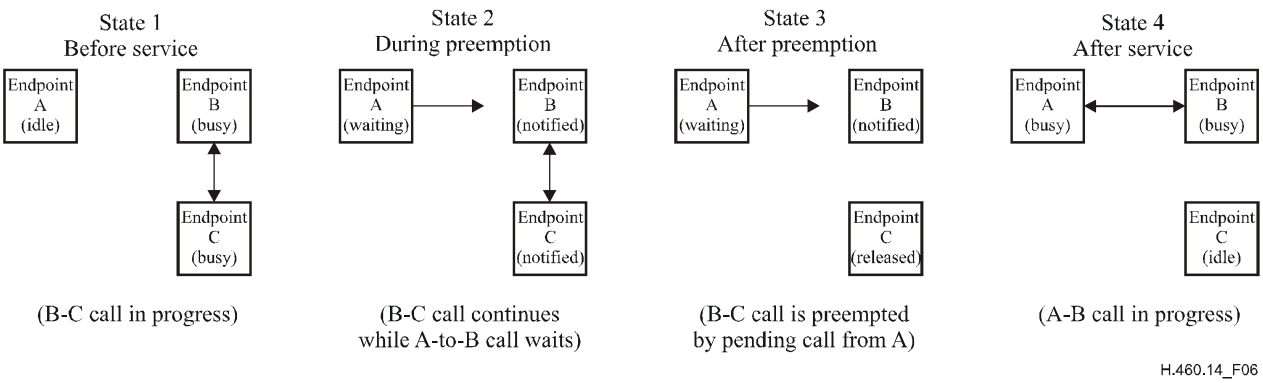


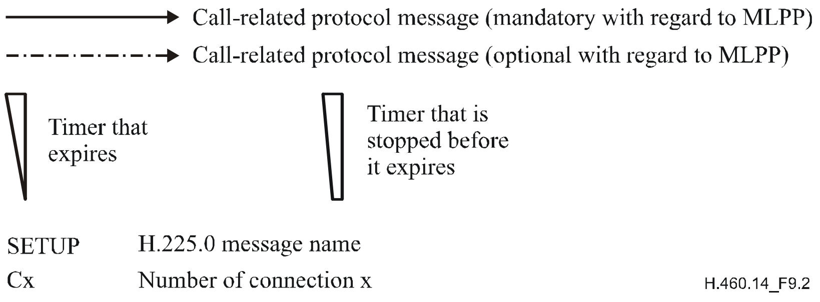
Figure 6/H.460.14 – Operational model for MLPP

NOTE – As defined in clause 4, "Preemption in Progress" includes states 2 and 3 in Figure 6.

9.2 Signalling flows

This clause describes some typical message flows for MLPP. The following conventions are used in the figures of this clause.

The following notation is used:



9.2.1 Successful MLPP – direct endpoint call signalling

Figures 7 and 8 show example signalling flows for a successful MLPP invocation and operation for the direct endpoint call signalling case.

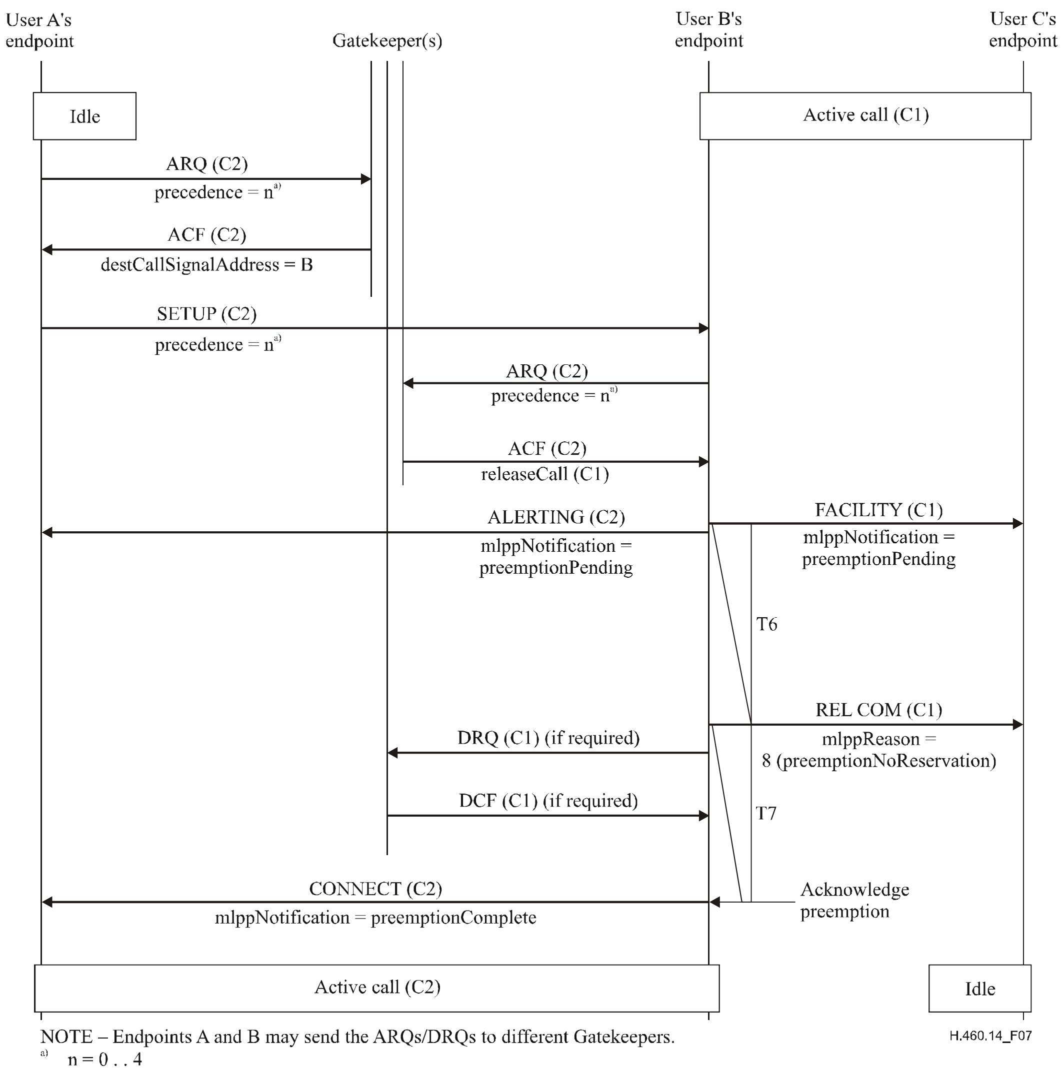
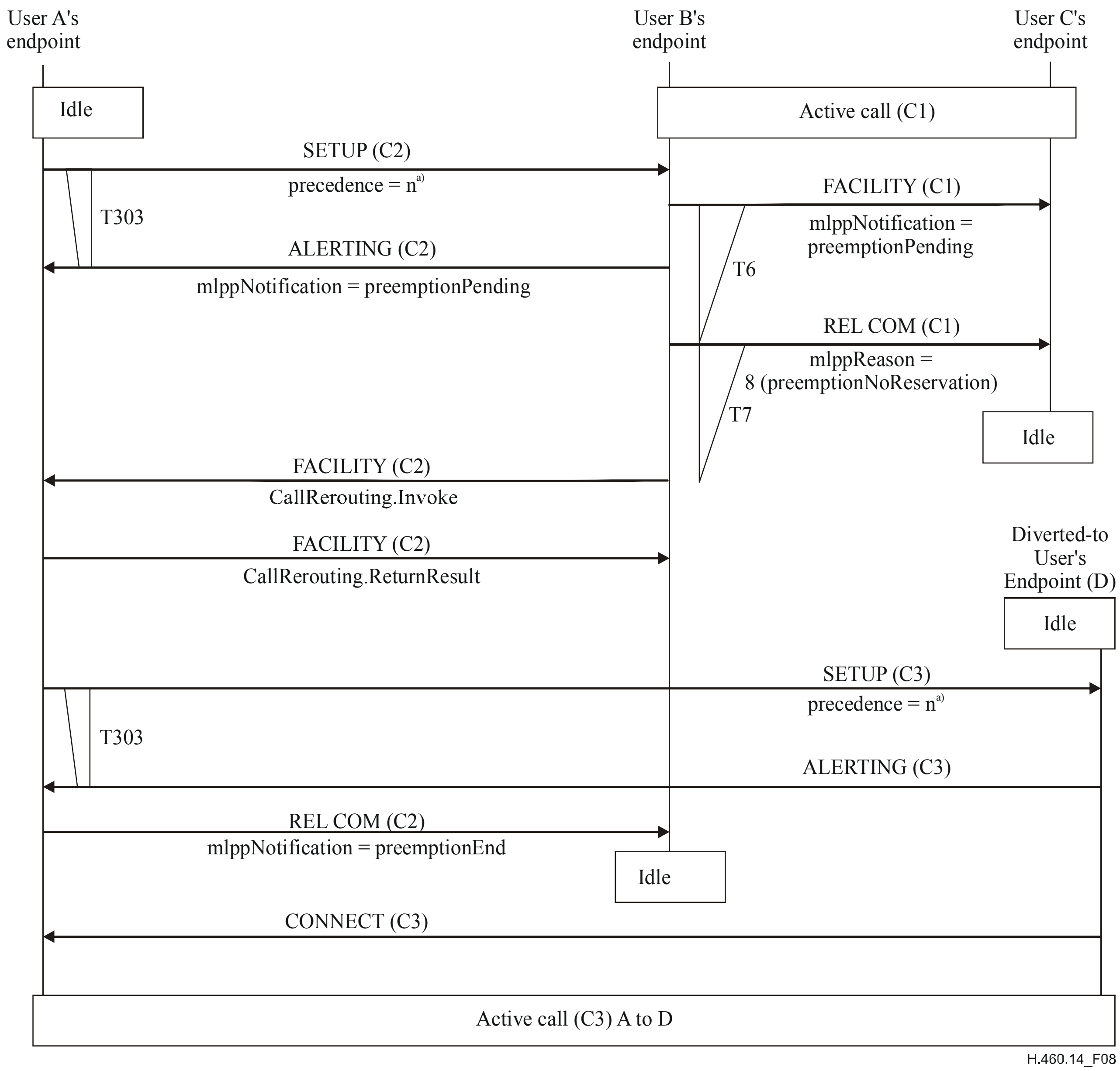


Figure 7/H.460.14 – Example message flow for successful MLPP – direct endpoint call signalling, established call preempted



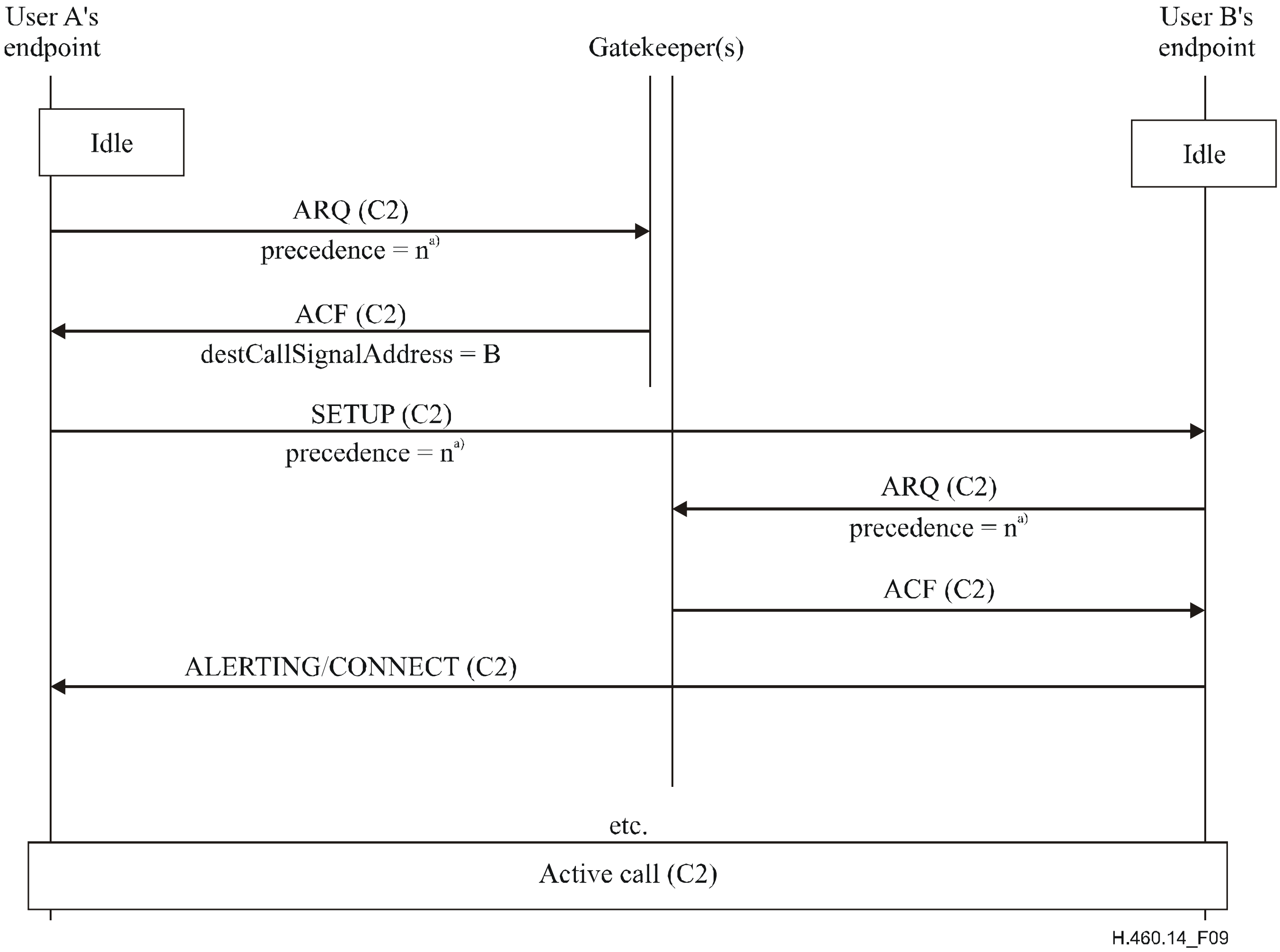
a) n = 0 . . 4

RAS signalling not shown – same as previous figure

Figure 8/H.460.14 – Example message flow for successful MLPP – direct endpoint call signalling, with timeout of acknowledgement and diversion

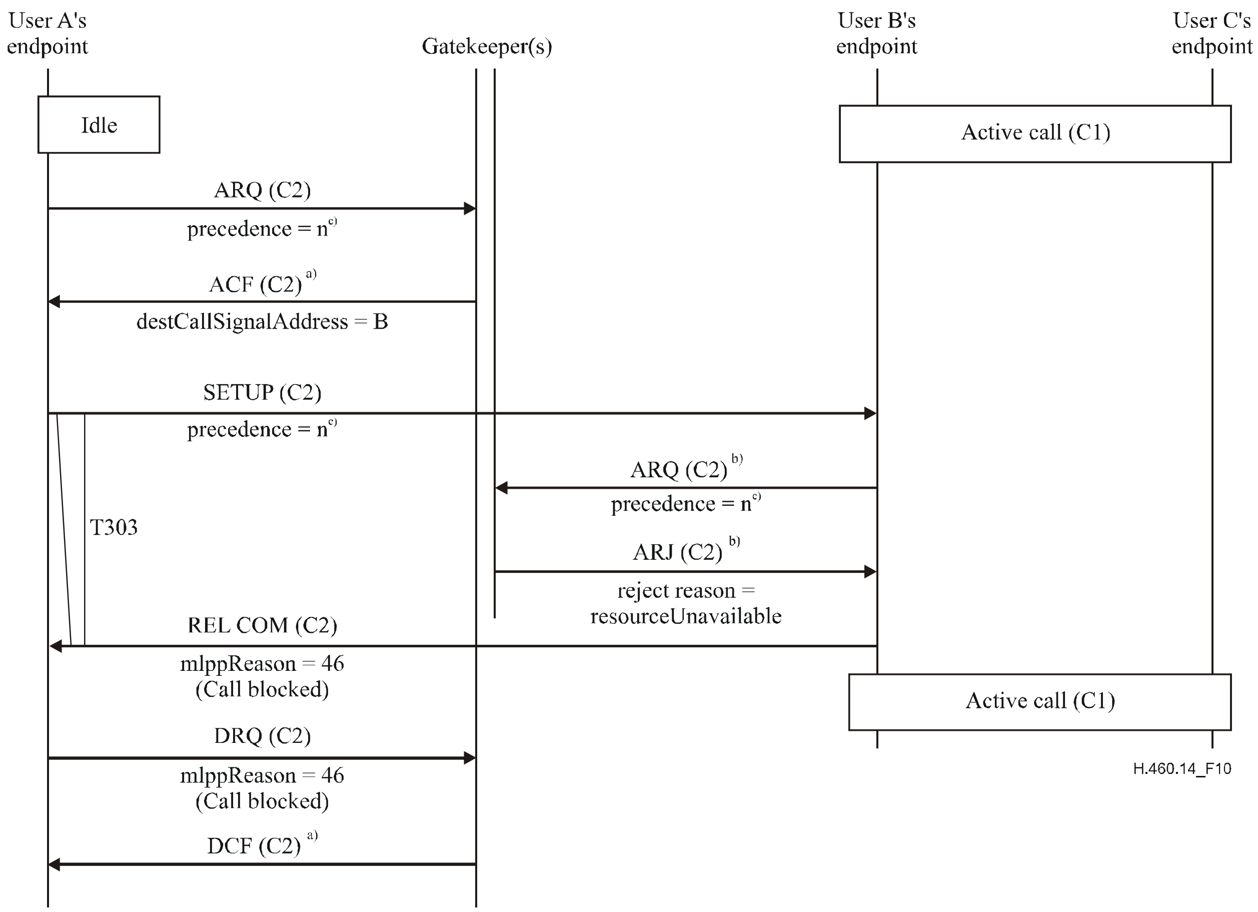
9.2.2 MLPP call without preemption – direct endpoint call signalling

Figures 9 and 10 show example signalling flows for MLPP invocation to an idle endpoint in the direct endpoint call signalling case. (It should be emphasized that, in the case shown in Figure 9, although the MLPP service is considered "unsuccessful" from the protocol viewpoint, the call setup is successful from the service operation viewpoint.)



a) n = 0 . . 4

Figure 9/H.460.14 – Example message flow for unsuccessful MLPP – direct endpoint call signalling with User B not busy



a) The gatekeeper may return ARJ if it knows that the active call is not preemptable.

b) Endpoint B may immediately return REL COM without first sending ARQ if it knows that the current call cannot be preempted.

c) n = 0 . . 4

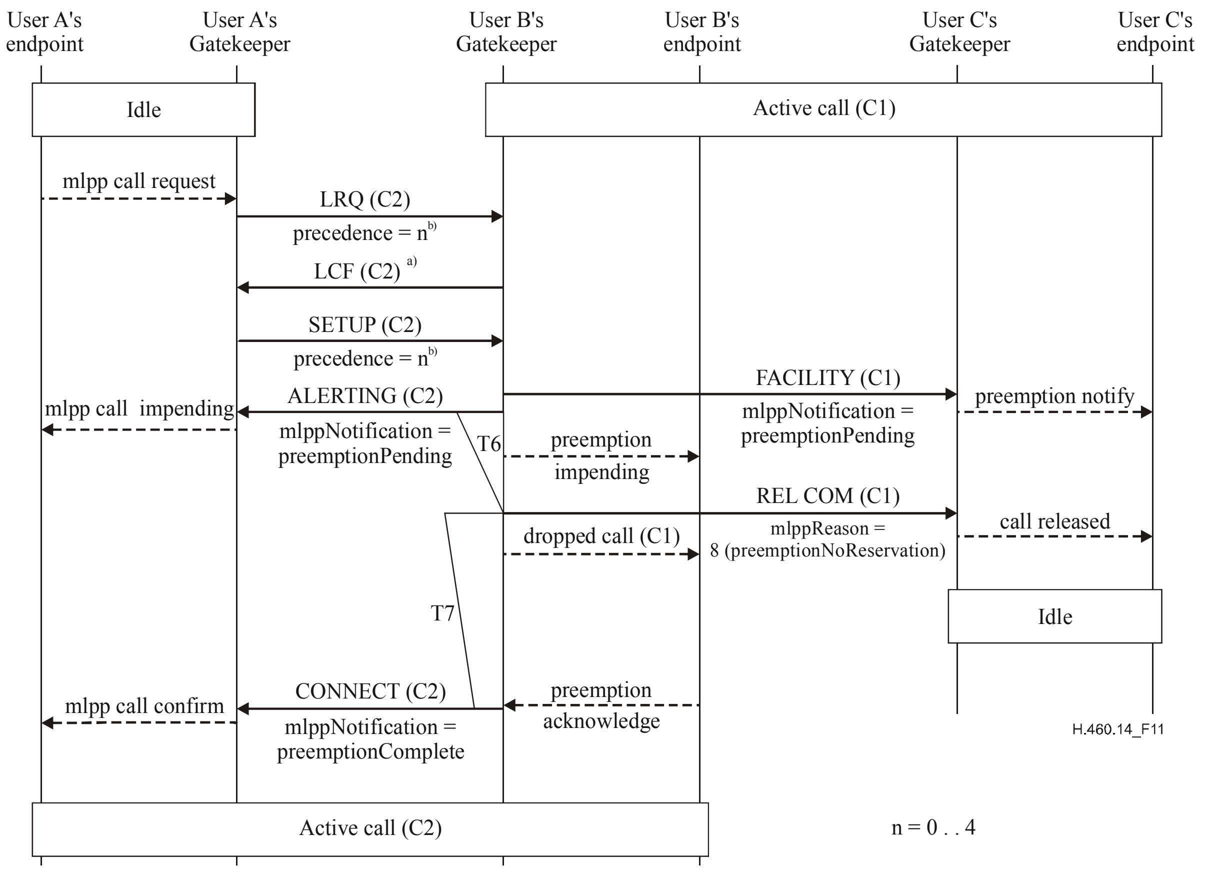
Figure 10/H.460.14 – Example message flow for unsuccessful MLPP – direct endpoint call signalling with insufficient precedence level (without alternate party diversion)

In the case shown in Figure 10, if endpoint B knows that it has no preemptable facilities and that there is no alternate party diversion, it may reject the call setup by sending the Release Complete without first sending the ARQ.

9.2.3 Successful MLPP – Gatekeeper – routed call signalling, stimulus signalling to endpoints

Figure 11 shows an example of the signalling flows for a successful MLPP invocation and operation with terminal endpoints A, B, and C not being capable of MLPP according to this Recommendation (e.g., H.323 terminals with stimulus feature control). In this example, a Gatekeeper or a proxy acts on behalf of each endpoint MLPP.

The terminal interfaces at endpoints A, B, and C are shown to illustrate the examples only. These interfaces are out of the normative scope of this Recommendation. Only the interfaces between each Gatekeeper/proxy and its associated endpoint are part of the normative scope of this Recommendation.



a) LRJ (C2) with admissionRejectReason = resourceUnavailable if call cannot be accommodated.

b) n = 0 . . 4

Figure 11/H.460.14 – Example message flow for successful MLPP – Gatekeeper-routed call signalling, non-standard signalling to endpoints

9.2.4 Successful MLPP – GK-routed call signalling, standardized functional signalling to endpoints

In the case of functional signalling to an endpoint, the Gatekeeper to Gatekeeper interactions are as shown in Figure 11 and the Gatekeeper to Terminal interactions are as shown in Figure 7 through Figure 10. In this case, either the Gatekeeper or the endpoint may perform the MLPP operations, for example, control of preemption, timing, and initiation of diversion.

9.3 Call states

The following states are defined only for the purpose of supporting the procedural descriptions and figures in clauses 8.2 and 10. An implementation is not required to use these actual states.

9.3.1 Call states at endpoint A

The procedures for endpoint A are written in terms of the following conceptual states existing within the MLPP signalling entity in association with a particular call.

MLPP state	Description
MLPP-Idle	This state exists if MLPP is not active.
MLPP-Wait-Ack	This state exists after an MLPP request while waiting for a response.

9.3.2 Call states at endpoint B

The procedures for endpoint B are written in terms of the following conceptual states existing within the MLPP signalling entity in association with a particular call.

MLPP state	Description
MLPP-Idle	This state exists if MLPP is not active.
MLPP-Dest-Notify	This state exists after an impending preemption warning is given while waiting for the preemption to occur.
MLPP-Wait-for-Ack	This state exists after releasing the first call and waiting for the called user to acknowledge the preemption.

9.3.3 Call states at endpoint C

The procedures for endpoint C are written in terms of the following conceptual states existing within the MLPP signalling entity in association with a particular call.

MLPP state	Description
MLPP-Idle	This state exists if MLPP is not active.

9.4 Timers

The following timers are required for the implementation of MLPP. Depending on the signalling model used, they may be implemented in endpoints or in controlling gatekeepers.

9.4.1 Origination timers

None, other than those defined in ITU-T Rec. H.225.0.

9.4.2 Destination timers

- **Timer T6**

  Timer T6 controls the delay between an impending preemption warning notification and the forced release of the established call.

  Timer T6 should have a value not greater than 10 seconds. Immediate release is achieved by setting this timer to 1 second (allowing time for the notification).

- **Timer T7**

  Timer T7 controls the wait for the called party to acknowledge (and accept) the preemption. Upon expiry, diversion to an alternate party occurs, if one has been designated.

  Timer T7 should have a value of 4-20 seconds.

10 Specification and Description Language (SDL) diagrams for MLPP

The functional signalling procedures for MLPP signalling entities are described in SDL form in Figures 13 through 16. The SDLs only show MLPP specific information transported on an H.225.0 connection. H.245 procedures (e.g., terminal capability exchange, master/slave determination, opening and closing of logical channels, etc.) are not shown. RAS signalling is not shown. In addition, interactions with other services are not shown.

In case of a conflict between SDLs and the text within the other clauses of this Recommendation, the text shall take precedence.

The symbols used in the following SDLs, irrespective of the direction of input and output signals, are defined in Figure 12.

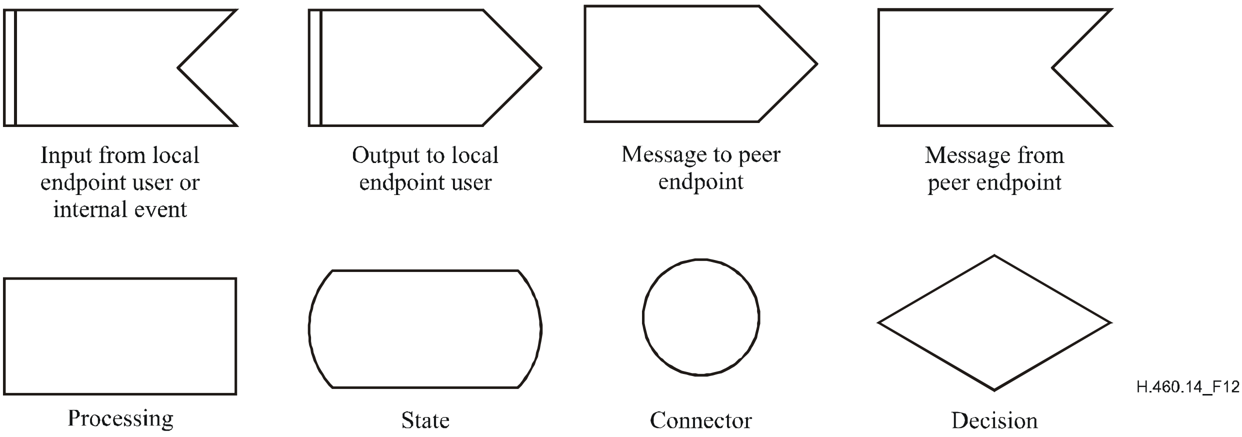


Figure 12/H.460.14 – SDL symbols

10.1 Behaviour of User A's endpoint

Figure 13 shows the behaviour of user A's endpoint.

Input signals from the left and output signals to the left represent:

- inputs from or indications and notifications to the user A;
- internal signals, e.g., timer expiry.

Input signals from the right and output signals to the right represent:

- messages from and to the called peer service control entity (i.e., in User A's Gatekeeper or User B's endpoint or Gatekeeper) which carry MLPP control information.

10.2 Behaviour of User B's endpoint

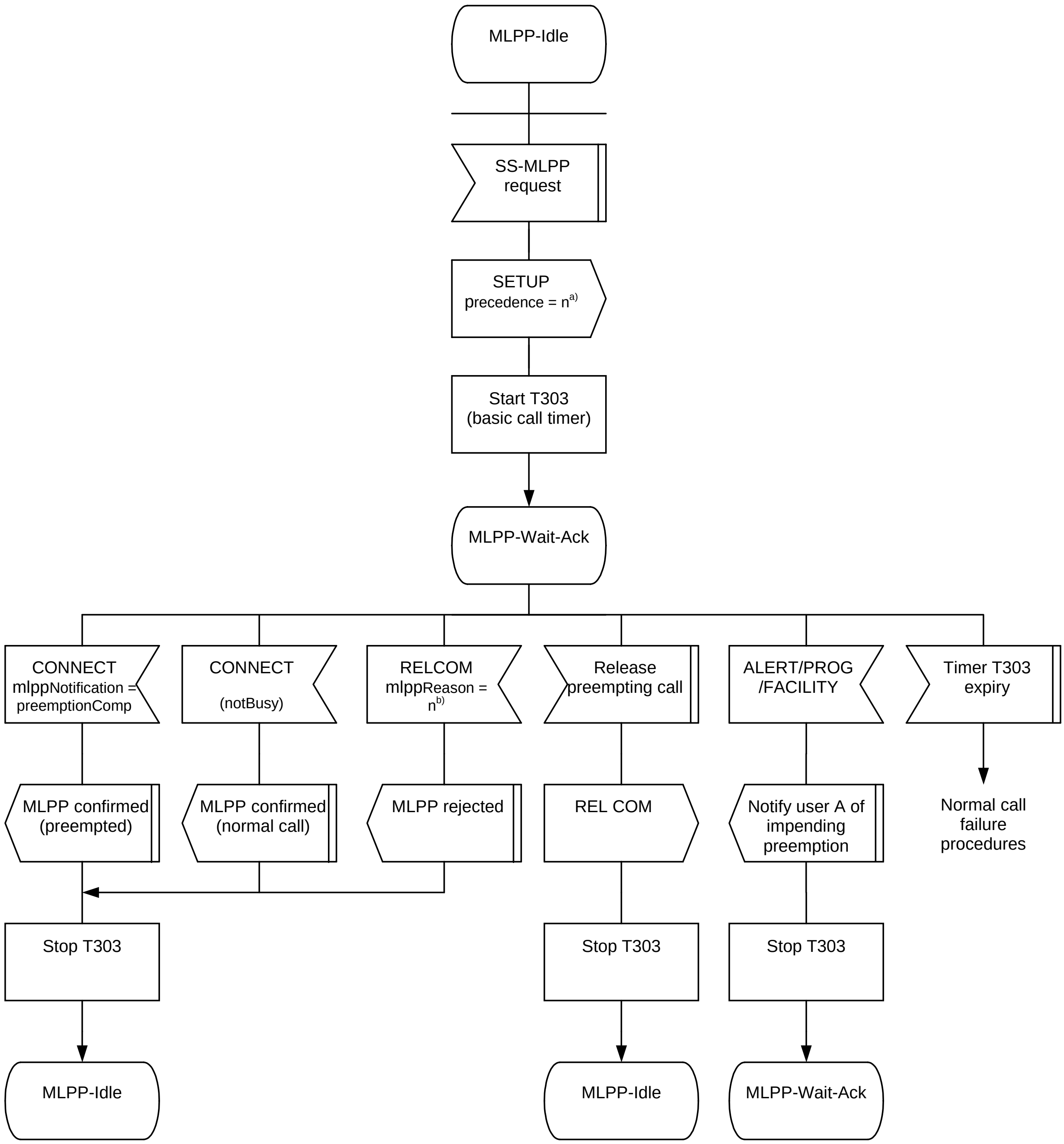
Figures 14 and 15 show the behaviour of User B's endpoint.

Input signals from the left and output signals to the left represent:

- messages from and to the calling peer service control entity (i.e., in User B's Gatekeeper or User A's endpoint or Gatekeeper) which carry MLPP control information;
- inputs from and indications and notifications to the called user (User B);
- internal signals, e.g., timer expiry.

Input signals from the right and output signals to the right represent:

- messages from and to the unwanted user's peer service control entity (i.e., in User B's Gatekeeper or User C's endpoint or Gatekeeper) which carry MLPP control information.



a) n = 0 . . 4

b) n ∈ MlppReason

Figure 13/H.460.14 – Endpoint A SDL

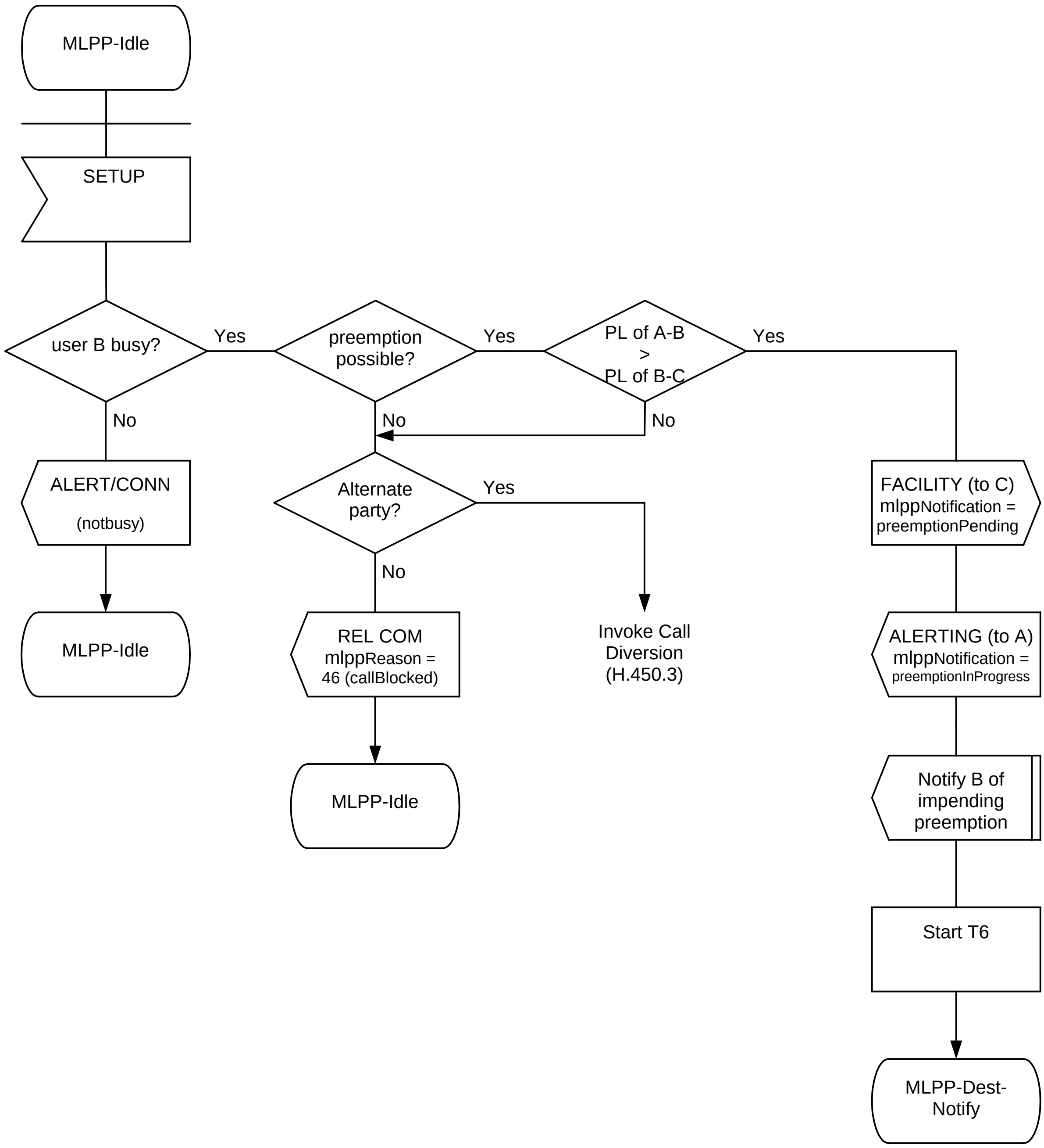


Figure 14/H.460.14 – Endpoint B SDL (*sheet 1 of 2*)

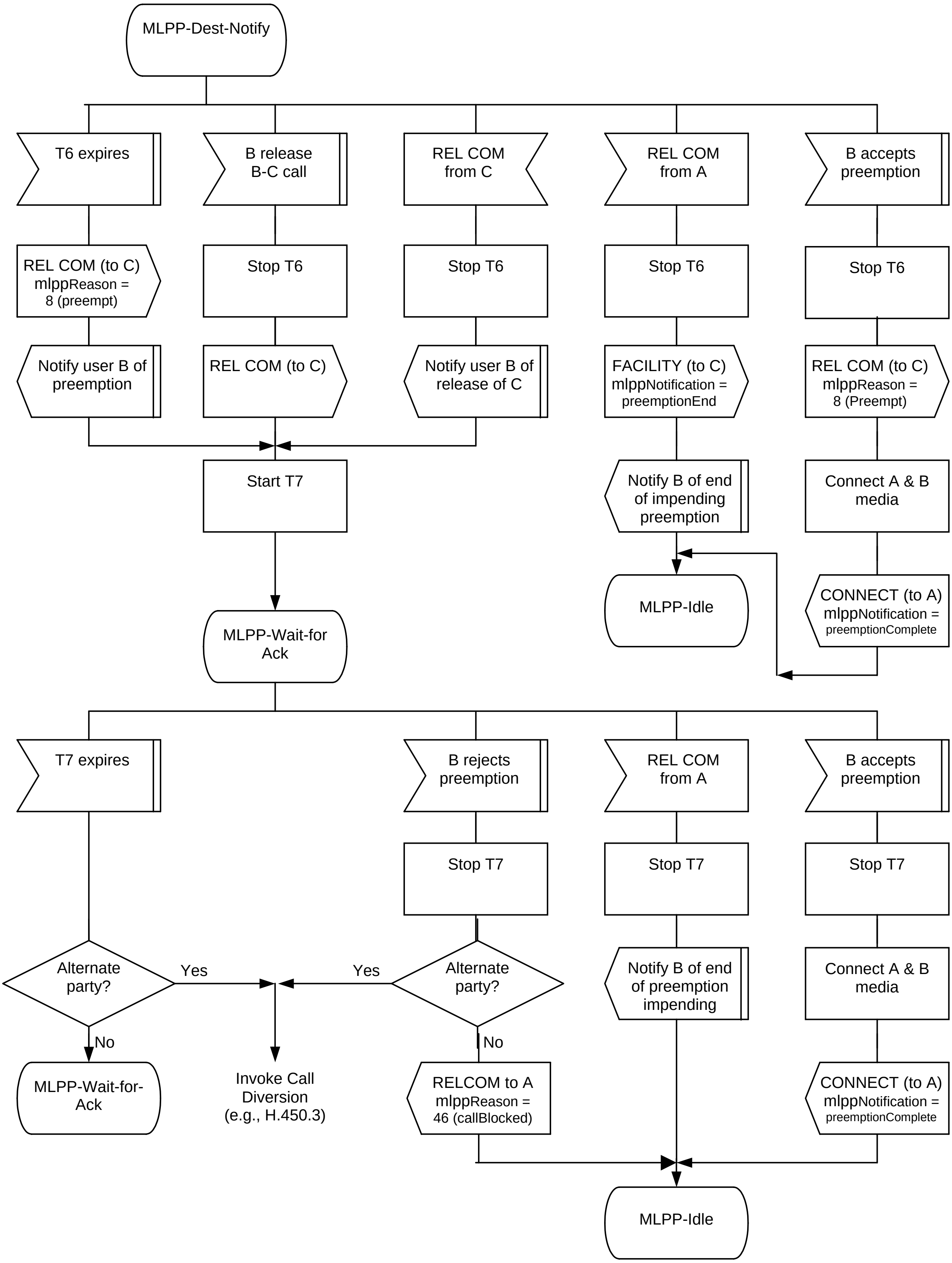


Figure 15/H.460.14 – Endpoint B SDL (*sheet 2 of 2*)

10.3 Behaviour of User C's endpoint

Figure 16 shows the behaviour of User C's endpoint.

Input signals from the left and output signals to the left represent:

- messages from and to the peer service control entity (i.e., in User C's Gatekeeper or User B's endpoint or Gatekeeper) which carry MLPP control information.

Output signals to the right represent:

- indications or notifications to the unwanted user (User C).

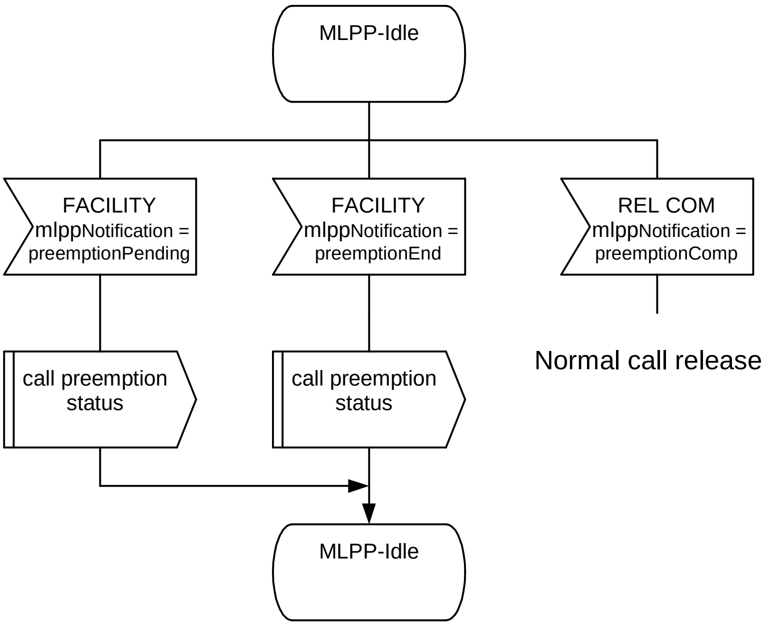


Figure 16/H.460.14 – Endpoint C SDL

11 Protocol interactions with other endpoint features

When other supplementary services are provided according to one or more of the following methods, the interactions of MLPP with the protocol used for those services shall be as follows:

11.1 Functional endpoints

Endpoints using H.450-series functional signalling for other services may utilize the procedures in this Recommendation to provide the MLPP service. They shall handle interactions with the protocols defined in the applicable Recommendations for those services as follows.

11.1.1 Call Transfer (SS-CT)

The following protocol interactions shall apply if SS-CT is supported in accordance with ITU-T Rec. H.450.2 and both SS-CT and MLPP are invoked on the same call:

If User A requests call transfer for two calls and MLPP is invoked on one or both calls, the actions of CT for transfer during alerting shall apply. The transferred-to endpoint may include a *callWaiting* invoke APDU (see ITU-T Rec. H.450.6) when sending the *callTransferSetup* return result APDU in an Alerting message to the transferred endpoint. The transferred-to endpoint may then also send a *remoteUserAlerting* invoke APDU in a Facility message to the transferred endpoint when the transferred-to user becomes not busy. If no *callWaiting* invoke APDU was sent, then also no *remoteUserAlerting* invoke APDU shall be sent. If the transferred-to user answers, a Connect message shall be sent to the transferred endpoint, but no MLPP **genericData** element shall be sent.

If the secondary call does not exist, the transferred endpoint may request MLPP against a transferred-to user by including in the Setup message an MLPP **genericData** element together with the *callTransferSetup* invoke APDU. The transferred-to endpoint shall then follow the procedures of 8.2.

11.1.2 Call Forwarding Unconditional (SS-CFU)

The following protocol interactions shall apply if SS-CFU is supported in accordance with ITU-T Rec. H.450.3 and both SS-CFU and MLPP are possible on the same call:

When executing call forwarding unconditional, the rerouting endpoint shall include in the Setup message to the diverted-to endpoint any **genericData** elements (including the ones for MLPP defined in this Recommendation) that were present in the Setup message received by the diverting endpoint, in addition to the *divertingLegInformation2* invoke APDU.

11.1.3 Call Forwarding Busy (SS-CFB)

The following protocol interactions shall apply if SS-CFB is supported in accordance with ITU-T Rec. H.450.3 and both SS-CFB and MLPP are possible on the same call:

When executing call forwarding busy, the rerouting endpoint shall include in the Setup message to the diverted-to endpoint any **genericData** elements (including any for MLPP) that were present in the Setup message received by the diverting endpoint, in addition to the *divertingLegInformation2* invoke APDU.

If a call including an MLPP **genericData** element arrives at a busy user who has activated SS-CFB, then SS-CFB shall be invoked.

11.1.4 Call Forwarding on No Reply (SS-CFNR)/Call Deflection (SS-CD)

No protocol interaction.

NOTE – This means that the rerouting endpoint does not include any MLPP **genericData** element in the new Setup message when executing call diversion (no reply/call deflection).

11.1.5 Call Hold

No protocol interaction.

11.1.6 Call Park/Call Pickup

No protocol interaction.

11.1.7 Call Waiting

No protocol interaction.

11.1.8 Message Waiting Indication

No protocol interaction.

11.1.9 Name Presentation

No protocol interaction.

11.1.10 Completion of Calls on Busy (SS-CCBS)/on No Reply (SS-CCNR)

No protocol interaction.

11.1.11 Call Offer (SS-CO)

The following protocol interactions shall apply if SS-CO is supported in accordance with ITU-T Rec. H.450.10 and both SS-CO and MLPP are invoked on the same call:

Endpoint A may include both the *callOfferRequest* and MLPP request in the Setup messages. In state MLPP-Wait-Ack, if a *callWaiting* invoke APDU is received in an Alerting or Progress message, endpoint A shall proceed with the Call Offer invocation procedures as defined in ITU-T Rec. H.450.10 instead of MLPP, as this occurs if the endpoint does not support MLPP. If any return error defined in this Recommendation is returned, endpoint A shall proceed with the procedures of this Recommendation.

Endpoint B shall respond positively as defined in this Recommendation rather than to the *callOfferRequest* invoke APDU. It shall respond to the *callOfferRequest* invoke APDU by returning a *callOfferRequest* return error APDU with error "*supplementatyServiceInteractionNotAllowed*" in the resulting Alerting or Connect message.

11.1.12 Call Intrusion (SS-CI)

No protocol interactions, since both services should not be invoked on the same call setup.

11.1.13 Common Information

No protocol interaction.

11.2 Stimulus-based endpoints

Feature interactions for stimulus-based endpoints shall be resolved in the controlling Gatekeeper or feature server. Generally, precedence calls should be forwarded, redirected, or transferred with their original precedence. In most cases, precedence calls follow the normal redirection procedures unless they are able to preempt an existing call at the called destination. Annex L/H.323 further describes the stimulus-based endpoint case.

11.3 Interworking with Switched Circuit Network

MLPP may interwork with corresponding supplementary services as defined by other standards by means of gateway interworking functions.

The specification of detailed gateway interworking procedures for MLPP is beyond the scope of this Recommendation and may be defined for various Switched Circuit Networks by other Recommendations.

Annex A/H.460.14

ASN.1 definition

```
MLPP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
     CallIdentifier,
     AliasAddress
FROM H323-MESSAGES;  -- defined in H.225.0, Annex H

MLPPInfo  ::=  SEQUENCE  -- root for MLPP data ASN.1
{
     precedence         MlppPrecedence     OPTIONAL,
     mlppReason         MlppReason         OPTIONAL,
     mlppNotification   MlppNotification   OPTIONAL,
     alternateParty     AlternateParty     OPTIONAL,
     releaseCall        ReleaseCall        OPTIONAL,
     ...
}

MlppPrecedence  ::=  ENUMERATED
{
     flashOverride (0),
     flash (1),
     immediate (2),
     priority (3),
     routine (4),
     ...
}

MlppReason  ::=  ENUMERATED
     -- Indicates reasons that call is refused or released.
{
     preemptionNoReservation (8),
     preemptionReservation (9),
     callBlocked (46),
     ...
}

MlppNotification  ::=  CHOICE
     -- Provides various notification events in Call Signalling messages
{
     preemptionPending       NULL,
     preemptionInProgress    NULL,
     preemptionEnd           NULL,
     preemptionComplete      NULL,
     ...
}

AlternateParty  ::=  SEQUENCE
{
     altID          AliasAddress,
     altTimer       INTEGER (0..255) OPTIONAL, --seconds
     ...
}

ReleaseCall  ::=  SEQUENCE
     -- Identifies other call to be preempted first
{
     preemptCallID      CallIdentifier,
     releaseReason      MlppReason,
     releaseDelay       INTEGER (0..255) OPTIONAL, -- seconds to wait
     ...
}

END
```

ITU-T Rec. H.460.21 (05/2006)

MESSAGE BROADCAST FOR H.323 SYSTEMS

Summary

This Recommendation defines a feature wherein H.323 devices may broadcast (using multicast) a message to one or more remote H.323 terminals, such as providing an "intercom" function for enterprise telephones, a "paging" service through an enterprise, or a notification system to geographically dispersed terminals. Since the method utilizes standard Internet multicast procedures, the feature may be used on a wide scale to reach any number of H.323 endpoints in a geographic region or even the entire world.

1 Scope

This Recommendation describes the signalling and procedures to provide a message broadcast feature for H.323 systems. The message broadcast feature is one wherein a message server or H.323 endpoint in the network transmits a message to one or more endpoints in a predefined multicast group. The message may result in alerting the user or playing audio to a speaker on the phone without alerting. Messages sent to an H.323 device may interrupt active communication or may be discarded, depending on priority. Messages are not limited to audio: messages may be audio, video, or text messages, the choices of which are negotiated through the procedures described herein.

These procedures use the H.323 Generic Extensible Framework (GEF).

2 References

2.1 Normative references

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

– ITU-T Recommendation H.225.0 (2006), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

– ITU-T Recommendation H.245 (2006), *Control protocol for multimedia communication*.

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

– ITU-T Recommendation H.460.1 (2002), *Guidelines for the Use of the Generic Extensible Framework*.

– ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

– ITU-T Recommendation X.691 (2002) | ISO/IEC 8825-2:2002, *Information technology – ASN.1 encoding rules – Specification of Packed Encoding Rules (PER).*

– IETF RFC 3376 (2002), *Internet Group Management Protocol, Version 3*.
– IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.
– IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*.
– IETF RFC 4103 (2005), *RTP Payload for Text Conversation*.

2.2 Informative references

– IETF RFC 3569 (2003), *An Overview of Source-Specific Multicast (SSM)*.

3 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ASM Any-Source Multicast

ASN.1 Abstract Syntax Notation One

GEF Generic Extensible Framework

GUID Globally Unique Identifier

PER Packed Encoding Rules

RAS Registration, Admission and Status

RCF Registration Confirm

RRQ Registration Request

SSM Source-Specific Multicast

4 Functional overview

Devices within an H.323 network that advertise support for the message broadcast feature do so through advertisements in the RRQ messages sent to the Gatekeeper. An endpoint may advertise that it is a receiver, a transmitter, or both. This allows a device to serve only to send out broadcast messages or perhaps provide intercom functionality as part of the other telephony functions.

Special devices in the network may serve as message broadcast servers and do not necessarily have to be H.323 entities: they only need to have the capacity to send media to multicast groups that may be properly received by H.323 entities operating in accordance with this Recommendation. Such servers are expected to share some information, such as multicast addresses and media attributes, with the Gatekeeper. How the Gatekeeper becomes aware of these servers or how information is shared with them is outside the scope of this Recommendation.

Gatekeepers have the ability to provide each endpoint with a list of multicast groups to which the endpoint may join. The list may be unique to each endpoint or a small group of endpoints, perhaps subdividing endpoints according to some logical association, such as a corporate department or geographic region. The way in which groups are defined and placed into the RCF is outside the scope of this Recommendation.

The addresses provided via the **groupAddress** field is a multicast address representing the multicast group (G). There is a second, optional, unicast address called **sourceAddress** representing the source (S) for media transmission.

When no particular source is specified for the multicast group (referred to as Any-Source Multicast or ASM), a receiving endpoint will accept message content from any device that transmits to that multicast group. No two entities should broadcast messages to the multicast group simultaneously, as that would induce some confusion. Nonetheless, such an event can occur and when it does, the message received from the highest priority group should be played, or from the first group to deliver a message in the case that the group priorities are the same. How the endpoint handles lower priority messages is implementation dependent; the device may choose to play the contents of the higher priority message, record and play the lower priority message after playing the higher priority message, discard the lower priority message, or take some other action.

When a source address is specified for the multicast group (referred to as Source-Specific Multicast or SSM), the endpoint accepts message content only from the source IP address specified. IGMPv3 and MLDv2 both provide mechanisms to allow the endpoint to signal to the network its desire to join the multicast group (S, G). By using SSM, a network administrator can better control the transmission of broadcast messages by restricting transmission to a small set of broadcast servers.

Endpoints may serve as receivers (most common), transmitters, or both.

Figure 1 depicts a network with a server transmitting a media flow to a multiplicity of H.323 terminals and gateways.

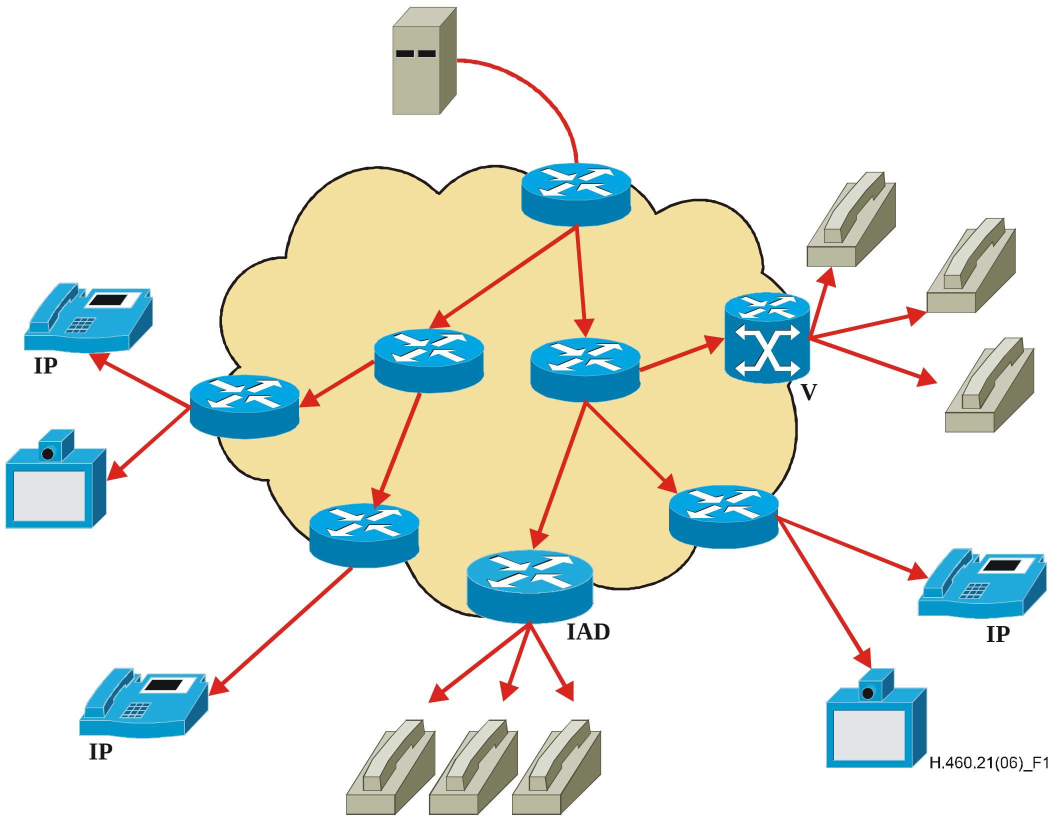


Figure 1/H.460.21 – Multicast message delivered to endpoints

5 Message content

Since there may be dozens, hundreds, or tens of thousands of devices that join a multicast group in order to receive broadcast messages, it is impractical to attempt to negotiate media capabilities with all of these devices in order to discover a common subset. As such, all devices that adhere to this Recommendation shall support, at a minimum, G.711 A-law and G.711 μ-law and shall be prepared to receive messages in either encoding with up to 240 samples (30 ms) of audio per packet. Devices should support RFC 4103 in order to receive broadcast text messages at a rate up to 30 characters per second.

The message content shall be streamed to the endpoint via RTP. However, since messages are intended to be relatively short and transmitted infrequently, the use of RTCP is not considered useful and shall not be employed with this feature.

NOTE – H.323 endpoints may indicate a language preference for broadcast messages it receives by including an ordered list of language preferences in the RRQ message transmitted to the Gatekeeper.

6 Message priority

In some cases, messages should not disrupt users on a call and there are other cases when users should be alerted. The **alertUser** field serves to provide guidance.

When the **alertUser** field is set to TRUE, the receiving H.323 device shall alert the user to the message as if it were an incoming call (e.g., ring the phone). If the H.323 device is engaged in a call, the message shall be delivered to the user, perhaps replacing one media stream for another. If the **alertUser** field is FALSE, the message should either be discarded or, if possible, played to the user interface (speaker or display) without alerting the user. In the case that the H.323 device is actively engaged in a call and the **alertUser** field is FALSE, the message should be discarded or recorded for later playback. The choice in behaviour is left to the implementer.

The **priority** field is used to provide guidance in dealing with multiple messages that may arrive at the same time or overlap in time. Once an endpoint starts delivering a message, the message should not be interrupted by another message unless that other message has a higher priority value. The lower the numeric value of the **priority**, the higher the priority (i.e., 0 is the highest priority).

User actions may disrupt message delivery. For example, if a departmental page is being delivered to the phone's speaker and the user lifts the handset on the phone to place a call, the message should stop playing unless the **alertUser** field is set to TRUE. In that case, it should continue delivery unless deliberately stopped. Methods for control of delivery and termination of delivery through the user interface are outside the scope of this Recommendation.

7 Gateway considerations

A gateway is a special device in that it has the capacity to reach a multiplicity of users, though presenting itself as a single H.323 entity to the Gatekeeper. The behaviour a gateway takes when it receives a message should be parallel to that of other H.323 devices. For example, if it receives a message for a group for which the user should be alerted, the gateway should attempt to alert users connected to the Gateway. For small gateway devices with ports that connect directly to analog phones, for example, alerting all of the phones is straightforward. However, for larger gateways that are connected to the PSTN without a well-defined set of "users", alerting this ambiguous group of users is impossible. In such a case, the Gateway may be provisioned with certain actions to take, such as calling phone numbers in a certain locality. In any case, the procedures that are followed by such Gateways are outside the scope of this Recommendation.

8 Capability advertisement

The message broadcast feature shall be advertising using the Generic Extensible Framework with the following feature identifier (see Table 1):

Table 1/H.460.21 – Message broadcast feature

Feature name:	Message Broadcast
Feature description:	This feature allows an H.323 endpoint to receive broadcast messages sent to groups of H.323 devices from another device on the network.
Feature identifier type:	Standard
Feature identifier value:	21

There is only one parameter defined for the message broadcast feature, as shown in Table 2. The specific SEQUENCEs to be sent in the RRQ and RCF messages are defined in the ASN.1 in Annex A.

Table 2/H.460.21 – Message broadcast feature parameter

Parameter name:	MessageBroadcastParameter
Parameter description:	This parameter holds the aligned variant PER encoding of ASN.1 definition found in Annex A.
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	Raw
Parameter cardinality:	Once and only once

8.1 Endpoint advertisement

Endpoints capable of supporting the message broadcast feature shall advertise that capability in the **featureSet.supportedFeatures** field of the RRQ message sent to the Gatekeeper. The MessageBroadcastParameter parameter shall contain a **CapabilityAdvertisement** SEQUENCE. Support for the message broadcast feature shall not be advertised in lightweight RRQ messages.

The endpoint shall advertise its receive capabilities and indicate the maximum number of multicast groups to which it can join via the **receiveCapabilities** field. The endpoint may include **receiveVideoCapability**, **receiveAudioCapability**, and **receiveDataApplicationCapability** capabilities as elements of **receiveCapability**. The use of other capability types is for further study. Gatekeepers in receipt of a capability other than these types or for a specific media type it does not support shall ignore the capability.

Different endpoint may advertise, for example, that they can receive G.711 A-law with a different number of samples per packet than another endpoint. However, if an endpoint advertises that it can receive G.711 A-law with 60 ms of audio per packet, the media stream may still contain only 30 ms (as indicated in clause 5) in order to accommodate all endpoints in the group.

Transmitters include the **transmitCapabilities** in the capability advertisement found in the RRQ. Each multicast group is identified by a Globally Unique Identifier (GUID), the assignment of which is outside the scope of this Recommendation and is intended to be assigned by administrators or operators. The transmitter indicates the capability that it will use to transmit to that group and the source address it will use for the transmission. The Gatekeeper will take this into account when it compiles the list of **MessageBroadcastGroups** it sends to the endpoints, setting the capability according to the information supplied by the transmitter. In the event that two devices claim to be the transmitter and when using ASM, the Gatekeeper may choose to use the capabilities of the first transmitter for the group associated with a particular GUID. There cannot be two transmitters for any group when using SSM.

8.2 Gatekeeper acknowledgement

Gatekeepers supporting the message broadcast feature and in receipt of an RRQ from an endpoint may return an RCF message with a **genericData** field element populated with a **MessageBroadcastGroups** SEQUENCE that allow the endpoint to then join the indicated multicast groups.

This list may be common to all endpoints or unique to each endpoint. Since the **MessageBroadcastParameter** allows multiple multicast groups to be specified, it is possible to indicate an enterprise paging group, for example, and one or more departmental groups within the RCF.

The endpoints which act as receiving devices shall then join the multicast groups and be prepared to receive messages. If an endpoint cannot join a particular group due to lack of support for a particular media capability, for example, the endpoint shall ignore the group.

Message groups shall be ordered in priority order in order to guide the endpoint in determining which media stream to join without sorting the list of groups locally by the **priority** field. The **priority** field shall be used to determine which media stream takes precedence over another when playing one message when another is received. (Refer to clause 6.)

A Gatekeeper may provide a list with more broadcast message groups than the endpoint can join. In that case, the order shall determine which groups are joined.

When sending the **MessageBroadcastGroups** list to endpoints, it is generally unnecessary to include the **groupIdentifier** field since this is only useful for the transmitter. The transmitter, on the other hand, needs this information to discover the multicast address to which it may transmit messages and what capability shall be used to transmit to the group. While the sender proposed a media type in the RRQ, the Gatekeeper may override that capability based on capabilities of devices in the network or administrative policies.

The Gatekeeper shall also indicate whether ASM or SSM is used for any particular multicast group. This decision is a matter of provisioning and is outside the scope of this Recommendation.

The Gatekeeper may change the list of multicast groups from time to time via the RCF message sent in response to a normal RRQ or a lightweight RRQ. Endpoints should be prepared to leave and join multicast groups with each RCF message. However, the RCF should not contain a list of groups unless the list changes. To force the endpoint to leave all multicast groups, the RCF shall contain the message broadcast feature advertisement in **genericData**, but shall not include the **MessageBroadcastParameter** parameter.

Annex A/H.460.21

ASN.1 definitions

```
MESSAGE-BROADCAST DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
     MulticastAddress,
     UnicastAddress,
     Capability
          FROM MULTIMEDIA-SYSTEM-CONTROL;

CapabilityAdvertisement ::= SEQUENCE
{
     receiveCapabilities     ReceiveCapabilities OPTIONAL,
     transmitCapabilities    SEQUENCE SIZE (1..256) OF TransmitCapabilities
                             OPTIONAL,
     ...
}

ReceiveCapabilities ::= SEQUENCE
{
     capabilities       SEQUENCE SIZE (1..256) OF Capability,
     maxGroups          INTEGER(1..65535),
     ...
}

GloballyUniqueID ::= OCTET STRING(SIZE (16))

TransmitCapabilities ::= SEQUENCE
{
     groupIdentifer     GloballyUniqueID,
     capability         Capability,
     sourceAddress      UnicastAddress,
     ...
}

MessageBroadcastGroups ::= SEQUENCE SIZE (1..256) OF GroupAttributes

GroupAttributes ::= SEQUENCE
{
     priority           INTEGER(0..255),   -- 0 = high, 255 = low
     groupIdentifer     GloballyUniqueID OPTIONAL,
     capability         Capability,
     groupAddress       MulticastAddress,
     sourceAddress      UnicastAddress OPTIONAL,
     alertUser          BOOLEAN,
     ...
}

END
```

Cable Communications Systems

ITU-T Rec. J.260 (01/2005)

REQUIREMENTS FOR EMERGENCY/DISASTER COMMUNICATIONS OVER IPCABLECOM NETWORKS

Summary

This Recommendation defines requirements for preferential telecommunications over IPCablecom networks. The essential aspects of preferential telecommunications over IPCablecom that this Recommendation covers can be grouped into two areas: prioritization and authentication. These two areas include capabilities to support telecommunications in IPCablecom that may require preferential treatment (e.g., Telecommunications for Disaster Relief and Emergency Telecommunications Service).

The implementation of priority and authentication is necessary for the support of preferential telecommunications in IPCablecom networks. Introduction

Introduction

Emergency/disaster communications for authorized users play a vital role in the health, safety, and welfare of people in all countries. The common thread to facilitate emergency/disaster operations is the utility of assured capabilities for user-friendly emergency telecommunications that may be realized by technical solutions and/or administrative policy. The IPCablecom infrastructure offers an important resource for assured emergency/disaster communications.

Emergency/disaster situations can impact communications infrastructures. Typical impacts may include congestion overload and the need to re-deploy or extend communications capabilities beyond that covered by existing infrastructures. Even when telecommunications infrastructures are not damaged by these situations, demand for telecommunications resources soar during such events. Therefore, priority mechanisms are needed so that limited bandwidth resources can be allocated to authorized emergency workers.

Generally, when preferential or priority treatment telecommunication capabilities are offered, users of the service will be authenticated and authorized. Whether authentication and authorization are required or not is a national decision. However, without authentication and authorization, preferential treatment capabilities may be subject to abuse by non-authorized individuals.

This Recommendation defines requirements for authentication and priority mechanisms in IPCablecom networks to provide preferential/priority treatment to services that need or benefit from such treatment.

1 Scope

The objective of this Recommendation is to provide an initial set of requirements for preferential telecommunications within IPCablecom networks. Aspects of preferential telecommunications include provisions for Authentication and Priority (Special Handling). These requirements do not apply to ordinary emergency calls such as people calling police, fire department, ambulance, etc. This Recommendation defines requirements for capabilities which when implemented should help support emergency telecommunication services.

NOTE – Pre-emption requirements and authorization requirements are outside the scope of this Recommendation and are considered to be national matters.

2 References

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

2.1 Informative references

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

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

3 Definitions

This Recommendation defines the following terms:

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

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

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

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

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

3.6 label: An identifier occurring within or attached to data elements. In the context of preferential telecommunications it is an indication of priority. This identifier can be used as a mapping mechanism between different network priority levels.

3.7 off-net: Not on an IPCablecom network.

3.8 on-net: On an IPCablecom network.

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

3.10 preferential: A capability offering advantage over regular capabilities.

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

4 Abbreviations

This Recommendation uses the following abbreviations:

CM Cable Modem

CMS Call Management Server

MTA Media Terminal Adapter

PIN Personal Identification Number

PSTN Public Switched Telephone Network

5 Architectural cases for preferential telecommunications over IPCablecom networks

These architectural cases are defined in order to provide the different cases that need to be specified.

5.1 IPCablecom to/from PSTN

This case includes calls made from the PSTN (Off-Net) to the IPCablecom network (On-Net) as well as calls made On-Net to Off-Net.

5.2 On-net to on-net

These three cases include calls made from a user on an IPCablecom network to a user on the same (or another) IPCablecom network.

5.2.1 Intra-zone

Intra-zone defines calls that remain within the technical control of a single CMS.

5.2.2 Inter-zone, intra-domain

Inter-zone, intra-domain defines calls that remain within the domain of a single Kerberos realm, but travel beyond the technical control of one CMS.

5.2.3 Inter-domain

The inter-domain case is not within the current scope of this Recommendation.

6 Requirements for preferential telecommunications in IPCablecom

The following requirements are for authentication and prioritization capabilities within IPCablecom networks. This initial set of requirements can be implemented utilizing existing mechanisms or extensions to existing mechanisms found within IPCablecom and elsewhere. Future enhancements as well as internetworking details will await the work of other ITU-T Study Groups.

The requirements focus on call control but some of them might also apply to voice traffic as well. Whether mechanisms need to be developed for the voice traffic as well as the call control depend upon the methods used for the priority and authentication.

Ideally, all methods of priority treatment will be applied to a priority call. However, it is recognized that satisfying a subset of the below listed requirements will improve the access for preferential users and that a phased approach to implementation is desirable.

6.1 Requirements for authentication in IPCablecom networks

Users with priority, generally, will be authenticated[2] and authorized. Whether authentication for preferential users is required or not is a national matter. In the case where authentication is not required it is assumed that preferential users are authorized by default. Ideally, at least two authentication mechanisms will be supported in IPCablecom networks. Some services may require only one method, however:

a) One method of authentication of calls originating in an IPCablecom network will be available to a preferential user on any given IPCablecom user's equipment. One way this can be accomplished is by calling a special number and entering a personal identification number (PIN).

b) One method of authentication will be dependent upon the IPCablecom system's recognition of the preferential users' equipment. This authentication will only be available on particular pieces of equipment (e.g., phones, CM/MTAs) and may additionally require further mechanisms (e.g., smartcards, tokens, and/or a PIN). Smartcards specifications are outside the scope of IPCablecom.

6.2 Requirements for priority treatment in IPCablecom networks

1) Preferential users will receive priority treatment. This priority treatment can be provided in several ways.
   a) Priority access to the IPCablecom network: This priority access will be provided after a preferential user is authorized and occurs when initiating a call on an IPCablecom network.
   b) Signalling associated with call activation and call features for preferential users will receive priority handling relative to non-preferential users.
   c) Network resources will be provided to preferential users on a preferential basis whether originating on the IPCablecom network (on-net) or entering from another network (off-net).
   d) Calls originating in an IPCablecom network (on-net) with a priority label should receive priority at the gateways to other networks (e.g., to the PSTN).
2) A priority call originating in an IPCablecom network is required to have a label or some other indication identifying the call as one which should receive priority treatment.
3) Calls with the priority label will receive priority treatment within an IPCablecom network.
4) A gateway device (on the IPCablecom side) connecting an IPCablecom network to the PSTN is required to be able to read the label of a priority call and map this label into priority mechanisms existing in the PSTN. The intent is to preserve the special handling (if available) as the call proceeds on the PSTN.

   NOTE – Generally, for the PSTN only one level of priority is available.
5) A gateway device (on the IPCablecom side) is required to be able to read priority label(s) from the PSTN associated with the call and map this label to the appropriate priority label within the IPCablecom network.
6) The priority label of a call that transits an IPCablecom network is required to be preserved throughout an IPCablecom network.

---

2 Authentication is important for priority traffic for several reasons:

a) To avoid denial-of-service attacks by non-authorized use of the priority treatment;

b) To allow the QoS provisioning to take place giving priority to the authorized user;

c) To allow for billing and accounting.

7) A priority call in transit through an IPCablecom network will receive priority treatment in accordance with the capabilities of the IPCablecom network.

8) There will be a minimum capability of supporting one level of priority treatment within an IPCablecom network. Some national options may require more levels (e.g., five levels). National options may require that outside of a "Declared time of Disaster, Crisis or Emergency", no Priority level or indications are active in the network. The number of different labels within an IPCablecom network associated with priority treatment may be extensible (e.g., up to 256) to allow for future extensions.

9) Any call entering an IPCablecom domain with a priority label from a trusted network (e.g., from the PSTN) will receive priority treatment in the IPCablecom network. The definition of "trusted network" is outside the scope of this Recommendation.

BIBLIOGRAPHY

T1* Technical Report T1.TR.79-2003, *Overview of standards in support of Emergency Telecommunications Service (ETS).*

* T1 standards are maintained since November 2003 by ATIS.

Telecommunications Network Management

ITU-T Rec. M.3350 (05/2004)

TMN SERVICE MANAGEMENT REQUIREMENTS FOR INFORMATION INTERCHANGE ACROSS THE TMN X-INTERFACE TO SUPPORT PROVISIONING OF EMERGENCY TELECOMMUNICATION SERVICE (ETS)

Summary

This Recommendation provides the basic functional requirements, framework, and use-cases for interchange of service management information across the TMN X-interface between a service customer and service provider, both officially authorized, associated with provision of Emergency Telecommunication Service (ETS). This capability is called the Emergency Telecommunication Service (ETS) Management Service (ETSMS).

Introduction

During catastrophic events, such as earthquakes, severe storms, floods, and civil unrest, governmental and other essential users of public telecommunications need a preferential telecommunication capability to support emergency and disaster relief operations. Telecommunication resources are often restricted during these serious events due to damage, congestion, and failures. Therefore, it is desirable to establish and manage telecommunication capabilities to support disaster relief operations that will provide a high probability of completion of emergency telecommunications. ITU-T Rec. E.106 [1] describes an International Emergency Preference Scheme (IEPS) for PSTN, ISDN, and PLMN telephony services to support emergency recovery activities during crises.

Certain international and national telecommunication capabilities will enable authorized users to have preferential access to telecommunication services and preferential processing of telecommunications to support recovery operations during emergency and disaster events. These capabilities, when provided nationally, are referred to as the Emergency Telecommunication Service (ETS). While some countries already have national preference schemes in existing telecommunication systems, the challenge at hand is provisioning appropriate priority mechanisms for a family of multimedia services in the newly emerging generation of packet-based networks, as well as ensuring effective interoperation with existing PSTN, ISDN, and PLMN emergency services, facilitating also international telecommunications when applying ITU-T Rec. E.106. Interchange of critical service management information could significantly benefit emergency recovery operations. Service management information associated with ETS operations needs to be shared between SP and SC authorized to manage emergency and disaster relief operations to ensure the best possible telecommunication support is provided under the stressful circumstances. The ETS Management Service (ETSMS) addressed by this Recommendation will provide this capability.

1 Scope

The subject of this Recommendation is the interface between a duly authorized service customer (SC) and a duly authorized service provider (SP) that is used to manage emergency telecommunication service (ETS) features. ETS features are used by emergency responders during disaster events for telecommunications to organize and coordinate activities for saving lives and restoring community infrastructure. The definition of actual ETS features and requirements are the subject of other Recommendations.

This Recommendation describes the ETS Management Service (ETSMS) and identifies functional requirements for interchange of critical service management information, which relates to ETS features, among TMNs across the X-interface of the service management layer as defined by ITU-T Rec. M.3010 [2]. The requirements described will enable authorized disaster response and recovery operations personnel, as SCs, to interact with SPs to share knowledge of the availability of services, configure services, and activate required services. Some aspects of the ETSMS may be used at any time independent of the occurrence of actual emergencies.

Other TMN Recommendations will cover the specific format and data elements as well as the protocols for interchange of management information across the X-interface for the ETSMS.

2 References

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

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

[2] ITU-T Recommendation M.3010 (2000), *Principles for a telecommunication management network*.

[3] ITU-T Recommendation M.3208.1 (1997), *TMN management services for dedicated and reconfigurable circuits network: Leased circuit services*.

[4] ITU-T Recommendation X.731 (1992) | ISO/IEC 10164-2:1993, *Information technology – Open Systems Interconnection – Systems management: State management function*.

[5] ITU-T Recommendation X.790 (1995), *Trouble management function for ITU-T applications*.

3 Terms and definitions

This Recommendation defines the following terms:

3.1 availability: The measure of ability of the network resources to support ETS or ETSMS features that could be used as activated or to be activated by authorized users supporting emergency and disaster relief operations.

3.2 degradation: A state of the ETS in which the quality of service level falls below a minimum threshold specified in the service level agreement between SC and SP.

3.3 ETS Management Service (ETSMS): A management service that provides capabilities for interchange of critical service management information, which is related to available ETS features, between service customers and service providers responsible for disaster relief operations to recover from catastrophic events.

3.4 failure: Loss of capability to support ETS communications or the ETSMS.

3.5 Service Level Agreement (SLA): A Service Level Agreement (SLA) is a formal negotiated agreement between two parties. It is a contract that exists between the Service Provider (SP) and the Service Customer (SC). It is designed to create a common understanding about service, quality, priorities, responsibilities, etc. SLAs can cover many aspects of the relationship between the SC and the SP, such as performance of services, customer care, billing, service provisioning, etc.

3.6 ETS network operator: An authorized organization that operates a telecommunication network and provides ETS features for ETS service users. An ETS network operator may be a SP and *vice versa*.

3.7 ETS service customer: A designated manager of the ETS features and the recognized user of the ETSMS. There may be different levels of SCs from national and regional down to the immediate local disaster area. The Service Level Agreement (SLA) for the ETS and ETSMS is between the SC and SP.

3.8 ETS service provider: An authorized service provider of the ETS features and the ETSMS.

3.9 ETS service user: The ETS service user (SU) is authorized by the SC to use the ETS features. The SU is not a user of the ETSMS.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ETS Emergency Telecommunication Service

ETSMS ETS Management Service

IEPS International Emergency Preference Scheme (E.106)

ISDN Integrated Services Digital Network

PLMN Public Land Mobile Network

PSTN Public Switched Telephone Network

SC (Authorized ETS) Service Customer

SLA Service Level Agreement

SP (Authorized ETS) Service Provider

SU (Authorized ETS) Service User

TMN Telecommunication Management Network

5 Conventions

Conventions used in use-case diagrams and the use of UML are imported from ITU-T Rec. M.3020.

6 ETSMS functional requirements

6.1 ETSMS framework

Disaster situations can strike unexpectedly anytime and anywhere. Recovery requires rapid response by local, regional, and national authorities, immediate reaction from utility service providers, and support from medical, recovery, fire, police, and construction resources. Effective communications are essential to facilitate the myriad of activities required for organizing and coordinating lifesaving efforts concurrent with re-establishing control in the disaster area and restoration of the community infrastructure. Effective telecommunication services are imperative to the success of disaster recovery and mitigation operations.

Emergency and disaster relief operations require extensive coordination and cooperation by organizations involved in restoring the infrastructure and for the well being of the society impacted. During these disaster situations, telecommunication services are often severely disrupted through facility damage as well as congestions due to significantly increased telecommunication traffic. Operations centres may be established or activated to coordinate the myriad of activities that are required to recover from the destruction, locate missing people, save lives, recover the infrastructure of the community, and restore normal living conditions for the population. ETS telecommunications to support these emergency recovery operations are given preferential access and processing treatment (e.g., as specified in ITU-T Rec. E.106).

The ETS Management Service (ETSMS) provides online interchange of critical telecommunications management information, which is associated in real time with provision of ETS features, and will significantly facilitate and benefit recovery operations. These interactions will more efficiently and effectively facilitate provisioning of essential telecommunications support by the authorized ETS Service Provider (SP), use of ETSMS by the authorized ETS Service Customer (SC), and use of ETS by the ETS Service User (SU). Specific requirements for interchange of important service management information for emergency and disaster relief operations are described in this Recommendation.

Figure 6-1 shows the reference interface X being addressed by this Recommendation. The X-interface is also referred to as the "Service Customer – Service Provider" interface and is used to convey information related to service management as defined in ITU-T Rec. M.3010. Within this Recommendation, the SC is the disaster response individual or function, such as an emergency operations centre, that is assigned responsibility to interface with the ETS management system. ETSMS enables interchange of service management information between SCs and SPs to assist disaster relief operations. The SP provides the ETSMS capability in support of the provisioning of ETS. The network management system and underlying element managers are components of the SP's operations support system. The ETS management system collects data from network and element managers and then makes available agreed upon service management data and information associated with the provision of ETS to the SC.

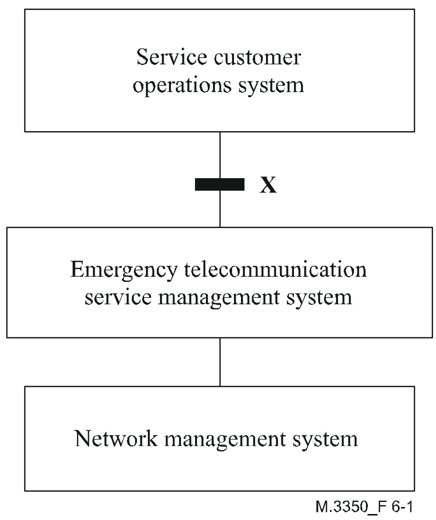


Figure 6-1/M.3350 – Reference interface

The authorized SP/SC/SU relationships for the ETS and ETSMS are illustrated by Figure 6-2. The SP provides ETSMS to support real-time, online interactions between the SC and SP to facilitate use of ETS for emergency operations.

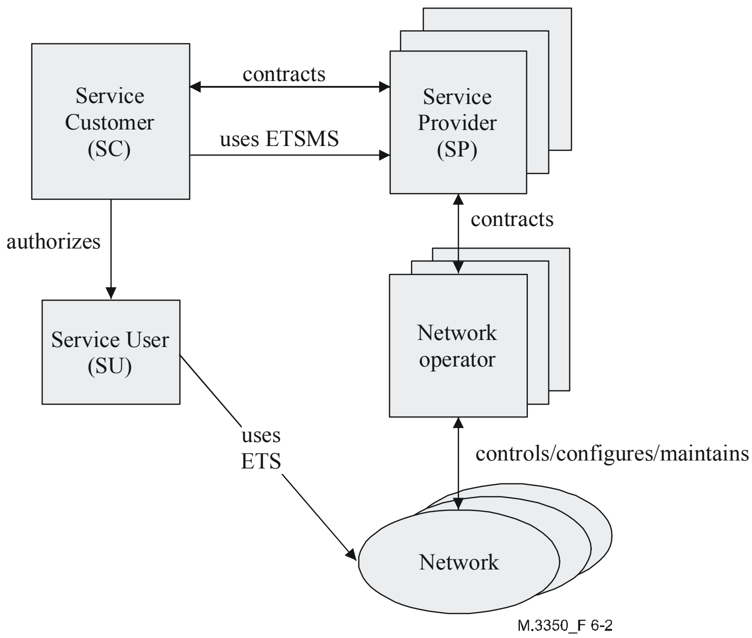


Figure 6-2/M.3350 – SP/SC/SU Roles for ETS and ETSMS

The SC is the party authorized to interface and interact with the ETSMS according to the established Service Level Agreement (SLA), contract, or service subscription established between the SC and SP. The SC then becomes the user of the ETSMS. The SC also identifies authorized SUs in cooperation with the appropriate authority. The authorized SUs will be registered with the SP using the ETSMS. The authorized SUs become the actual users of the ETS features. The SP may contract with a network operator, or the network operator functions may be provided as part of the SP's infrastructure. The network operator function is responsible for controlling, configuring, and maintaining the network infrastructure and resources.

The basic architecture of ETSMS across the X-interface is presented in Figure 6-3. It is adapted from the basic TMN architecture described in ITU-T Rec. M.3010.

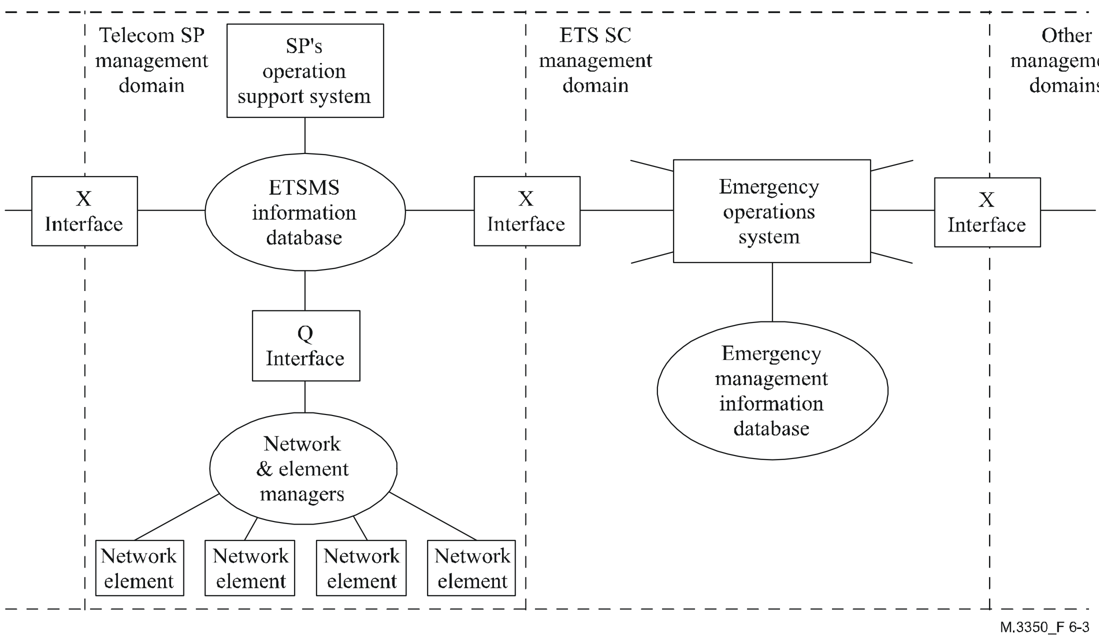


Figure 6-3/M.3350 – Architecture of ETSMS across the X-interface

Each of the management domains shown is considered to be an individual Telecommunication Management Network (TMN). The other management domains could be additional SPs that are supporting the ETS features and SCs that are authorized users of ETSMS. Each domain maintains its own emergency management or ETSMS database. The interchange of information and interactions between the SC and SP takes place across the X-interface. Only specific information that has been agreed upon between the SC and SP is shared using the ETSMS.

6.2 Basic requirements

The ETSMS is a service to support operations of the ETS features by SCs and SPs. It allows SCs to maintain knowledge of ETS availability and to provide reports to SPs of service problems and failures. It also allows SPs to provide SCs with reports of status and availability of ETS features.

Using ETSMS, SCs are able to register new authorized users or change their profiles across the X-interface at any time. If the ETS network features are not always active on a full-time basis, then the SC may use ETSMS to directly make online requests for the SP to activate ETS features as needed for areas that are affected by an emergency.

6.2.1 Management interactions

Table 6-1 lists service management interactions that could be conveyed across the ETSMS interface between SCs and SPs. This is the TMN X-interface for Service Management as defined by ITU-T Rec. M.3010.

Table 6-1/M.3350 – ETS management interactions across ETSMS interface

Initiator	ETS management interactions
Service Customer	Requests for activation of ETS features Modification of ETS parameters Requests for deactivation of ETS features Registration of authorized ETS users Modification of registered ETS user profile Deregistration of authorized ETS users Requests for ETS status Requests for specific on-demand reports about ETS Administration of alert triggers Administration of scheduled reports Submission of ETS trouble reports
Service Provider	ETS usage Reports ETS Security event alerts ETS degradation alerts ETS status change alerts

The ETSMS provides an interactive capability to manage the overall provisioning and maintenance of the ETS during a disaster relief operation. Clauses 6.2.1 and 6.2.2 provide a narrative description of the interactions passed across the interface. Clause 6.3 expands upon the narrative descriptions with specific use-cases that lead to the identification of specific functional requirements to be fulfilled by the ETSMS.

6.2.2 Interactions initiated by service customer

The following provides a narrative description of requests initiated by the SC and sent across the X-interface to the SP for action:

a) Requests for activation of ETS features – The ETS features may be available all the time or only when specifically requested by the SC. If ETS features are only activated upon declaration of an emergency, the SC would issue a request to activate certain ETS features or the total service. The situation may exist that only limited ETS features are always active and additional features are then activated upon request from the SC. Activation requests could include information about types of service to be activated, areas of service coverage, and categories of users to be supported by the ETS for the specific disaster instance.

b) Modification of ETS parameters – It may be necessary to change some parameters of the ETS features being used. For example, the area of coverage, service configuration, or types of service may need to be modified to accommodate specific situations that may arise.

c) Requests for deactivation of ETS features – The ETS features can be deactivated in networks that do not support full time activation of ETS features.

d) Registration of authorized ETS users – Only users specifically authorized by the appropriate authority are allowed to access the ETS features. The SC is responsible for registering the authorized users with the SP so that the SP can authenticate the users of the ETS before the request for access to ETS features is honoured. The registration information would include a profile of the level of service, types of service, and area of coverage that is authorized. In addition to registration of individual authorized users, specific access points and terminals could be registered with the profile of features that are allowed. The registration process may occur at any time, even when ETS is not activated.

e) Modification of registered ETS user profile – The parameters of a registered authorized user's profile can be changed at any time.

f) Deregistration of authorized ETS users – Registered authorized ETS users can be deregistered at any time.

g) Requests for ETS status – At any time, the SC can make a request to the SP to find out if specific ETS features are available. Some features may be active, but are not available because of limited network capacity. Other features may only be activated upon specific request by the SC as indicated in a) above. However, the SC could request the state of availability before an activation request is issued.

h) Requests for specific on-demand reports about ETS – The SC may request specific individual reports or sets of reports at any time. The SC may also terminate the delivery of a report at any time when justified.

i) Administration of alert triggers – Some reports that are to be provided by the SP will only be sent when triggered by specific events. The parameters for the event triggers can be administered through requests provided by the SC.

j) Administration of scheduled reports – Some reports that are to be provided by the SP will be delivered on an agreed upon schedule. The parameters for the schedule can be administered through requests provided by the SC.

k) Submission of ETS trouble reports – The SC experiencing a failure or problem with an ETS feature can issue a trouble report to the SP identifying the nature of the problem being experienced. A trouble report is essentially a request from the SC to the SP for corrective action to resolve the service problem. Upon receipt of a trouble report, the SP logs the report and initiates corrective action. During the corrective process and upon successful resolution of the trouble, the SP may provide status reports to the SC.

6.2.3 Management interactions initiated or provided by service provider

The following provides a narrative description of reports provided by the SP based upon the administered schedule or triggers. The reports are sent by the SP across the X-interface to the SC:

a) ETS usage reports – The SP reports on service usage could include statistical information about the actual usage of different types of service and areas of coverage for analysis purposes. These reports would be provided on a periodic schedule.

b) ETS security[3] event alerts – SP reports on security aspects when triggered by a specific event or change of status. The report could include identification of type of event, such as denial of service or attempted unauthorized access. The reports could include specific instances and locations of the security events.

c) ETS degradation alerts – SP reports on degradation of service when specific changes occur in the ETS quality of service level being provided. For example, a high volume of ETS traffic and/or limited bandwidth availability may lead to performance degradations. This type of alert will enable the SC and/or the SP to determine if some traffic types (e.g., video) or traffic levels should be controlled or limited.

d) ETS status change alerts – SP reports on service status would be provided when the state of service changes, e.g., when a service failure occurs. The reports may include the overall status of ETS service performance including information about types of service, areas of coverage, etc.

6.3 Business level requirements (use-cases)

Basic requirements (in text form) for ETSMS are provided in 6.2. Clauses 6.3 and 6.4 identify the associated use-cases with actor/role and resources. The goal of these clauses is to define system requirements for the Emergency Telecommunication Service Management System shown on Figure 6-1. The requirement of the system under development, that is, what functionality must be provided by the system, is documented in a use-case model that illustrates the system's intended functions (use-cases), its surroundings (actors), and the relationships between the use-cases and actors (use-case diagrams). Note that actors are not part of the system; they represent anyone or anything that must interact with the system.

6.3.1 Actors

The only actor defined is that of the Service Customer (SC) as identified in Figures 6-1 and 6-2.

6.3.2 Telecommunication resources

The telecommunication resources used to provide ETS and ETSMS are described in 6.1 (e.g., see Figures 6-2 and 6-3).

6.3.3 High-level use-case diagrams

This clause contains high-level use-case diagrams that summarize the functionality and interfaces of the Emergency Telecommunication Service Management System as shown on Figure 6-1. The use-case diagrams are organized along the lines shown in Table 6-1, i.e., use-cases initiated by the SC are depicted first followed by use-cases initiated by the SP. Use-case descriptions are provided in 6.4 for every use-case pictured in these high-level diagrams.

---

[3] The term "Security" is not yet defined officially in the ITU, except when used in the X-series of Recommendations.

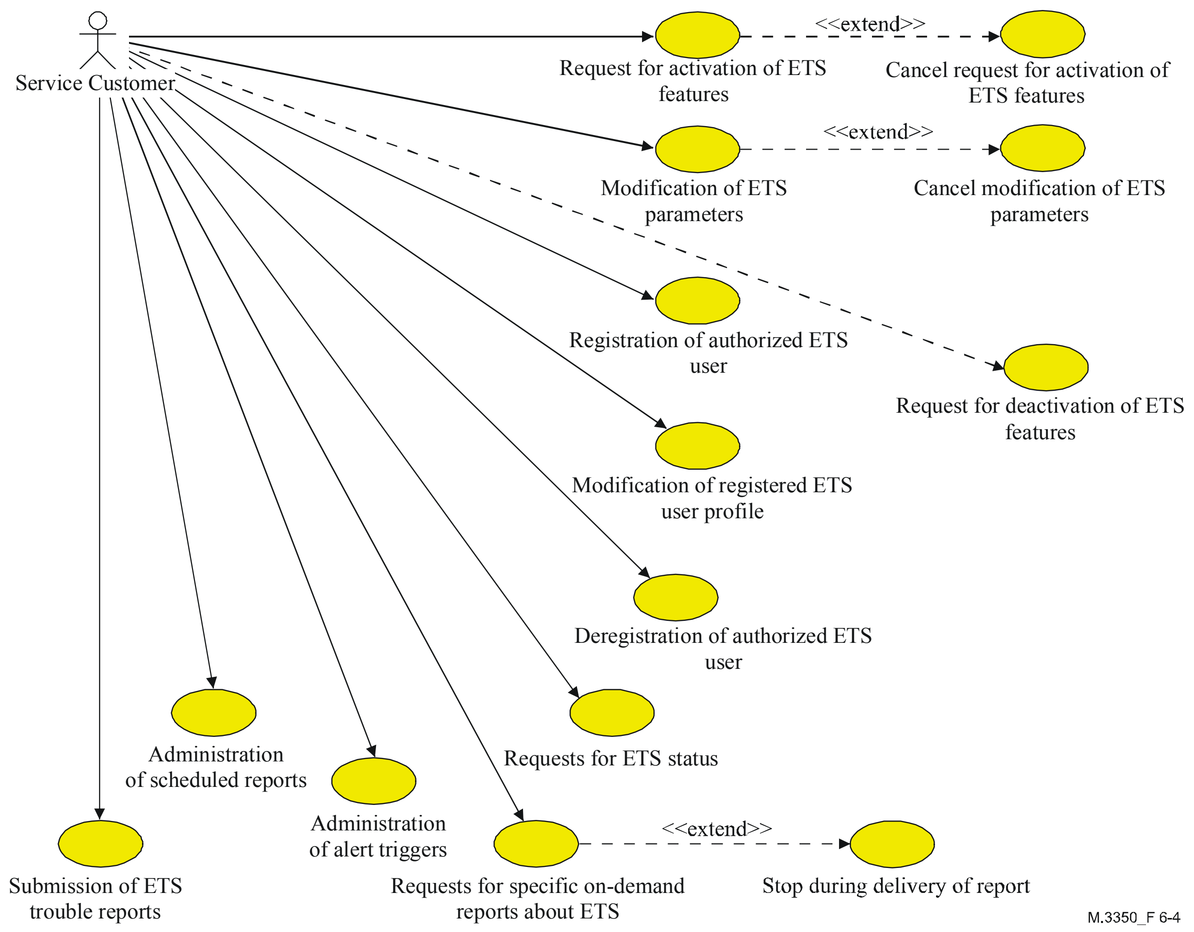


Figure 6-4/M.3350 – SC initiated use-cases

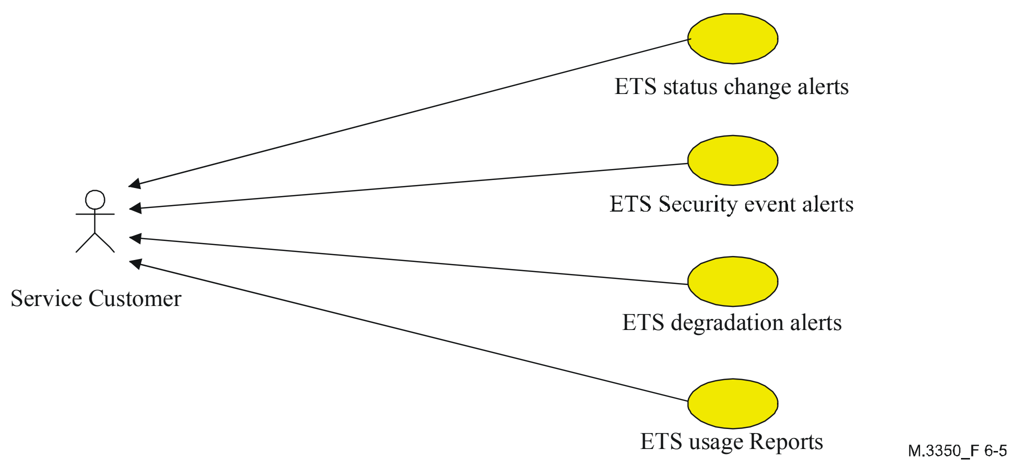


Figure 6-5/M.3350 – SP initiated use-cases

6.4 Specification level requirements

This clause contains textual details for each of the use-cases shown in the high-level use-case diagrams of the 6.3.3. The details are provided to clarify the roles of external actors and telecommunication resources and to refine the previous high-level use-case diagrams to a specification level. Use-case details include the following components:

Name	The name of the use-case (matches all drawing names).
Summary	A summary of the use-cases purpose and content.
Actor(s)	The names of actors involved in the use-case including role characteristic for each actor.
Assumptions	A description of the environment providing a context for the use-case.
Pre-conditions	A list of all system and environment conditions that must be true before the use-case can be triggered.
Begins when	The name of the single event that triggers the start of the use-case.
Description	The various tasks that make up the use-case, not necessarily in sequence. The description should reference any reuse of TMN functionality.
Ends when	The event(s) that signals that the use-case has terminated.
Exceptions	A summary list of all exception conditions and faults detected by the use-case during its operation.
Post-conditions	A list of all system and environmental conditions that must be true if the use-case has terminated without internal error.

The following subclauses provide the details for the use-cases shown on Figures 6-4 and 6-5.

6.4.1 Request for activation of ETS features

Name	Request for activation of ETS features
Summary	In situations where all ETS features are not always active, the SC activates one or more ETS features. The SP notifies the SC when the requested activation has completed. In terms of ITU-T Rec. X.731, *State management function*, activation of an ETS feature changes the administrative state of the ETS feature from "locked" to "unlocked".
Actor(s)	Service Customer (SC)
Assumptions	This use-case applies to situations where ETS is not always "available" for use and must be activated by specific request from the SC. The term "available" is used here to mean being made available administratively by the SP; it is not referring to the capability of the network to provide ETS. The ETS features are activated to enable authorized users to communicate for organizing and coordinating emergency recovery activities. Activated ETS features will allow registered users to access and use those ETS features. The ETS features can also be deactivated as requested by the SC (see 6.4.5). Only an authorized SC can request activation or deactivation.
Pre-conditions	An ETS network capability is in place and "available". The term "available" is used here to mean the network capability exists and is not experiencing a failure condition. A pre-defined ETS service contract has been established and the SC has been pre-authorized to perform this function.
Begins when	The SC requests activation of one or more ETS features.

Description	When the SC issues a request for ETS feature(s) activation, the SC will specify certain parameters as part of the request (e.g., identification of the ETS feature(s) to be activated, ETS parameter values associated with each ETS feature to be activated). Note that the SC may modify the ETS parameter values at a later time using the modification of ETS parameters use-case (see 6.4.3). When the requested ETS feature activation has completed, the SP notifies the SC that the requested ETS feature(s) are now "active".
Ends when	The SP notifies the SC that the requested ETS feature(s) is active.
Exceptions	– The ETS feature(s) was previously activated. – Requested feature or service not available. – Missing or incorrect parameter values. – The request originates from an unauthorized source. – A network problem exists.
Post-conditions	The state of the ETS feature(s) is "active", i.e., in terms of ITU-T Rec. X.731, its administrative state is "unlocked".

6.4.2 Cancel request for activation of ETS features

Name	Cancel request for activation of ETS features
Summary	The SC that submitted an earlier request for ETS feature activation (see 6.4.1) can cancel the request before the request is completed (as indicated by a completion notification issued by the SP).
Actor(s)	Service Customer (SC)
Assumptions	None
Pre-conditions	The SC has made an earlier request for ETS feature activation. Completion of the earlier request has not yet occurred, i.e., the request is in the "open/active" state as defined by Annex A.
Begins when	SC decides to cancel the original request.
Description	SC issues a cancellation request prior to completion of the earlier ETS feature activation request. If cancellation is successful, then SC is notified of success. If cancellation is unsuccessful, SC receives an exception report or confirmation that the original ETS feature activation request was successful.
Ends when	SC receives a success notification, an exception report, or an ETS feature activation confirmation.
Exceptions	– Original request has been completed (i.e., is in the "closed" state as defined by Annex A). – Too late to cancel. – The request originates from an unauthorized source.
Post-conditions	Original request is cancelled. A record of the original request and the cancellation may be kept available for future query (optional).

6.4.3 Modification of ETS parameters

Name	Modification of ETS parameters
Summary	The SC modifies one or more ETS parameters associated with an ETS feature.
Actor(s)	Service Customer (SC)
Assumptions	It may be necessary to change some parameters of the ETS features being used. For example, the area of coverage, service configuration, or types of service may need to be modified to accommodate specific situations that may arise. It is assumed that the state of the ETS feature for which ETS parameters are being modified is "active", however, it not necessarily assumed that activation/deactivation of the feature by the SC is allowed (see 6.4.1 and 6.4.5). Only an authorized SC can request modification of ETS parameters.
Pre-conditions	The state of the ETS feature for which ETS parameters are being modified is "active". A pre-defined ETS service contract has been established and the SC has been pre-authorized to perform this function.
Begins when	The SC requests modification of one or more ETS parameters associated with a specific ETS feature.
Description	When the SC issues a request for modification of ETS parameters, the SC will specify certain parameters as part of the request (e.g., identification of the ETS feature for which parameters are to be modified, new values for the ETS parameters to be modified, etc.). When the requested ETS parameter(s) modification has completed, the SP notifies the SC that the new ETS parameter value(s) that were requested are now in effect.
Ends when	The SP notifies the SC that the new ETS parameter value(s) are in effect.
Exceptions	– Missing or incorrect parameter values. – Requested feature not available. – The request originates from an unauthorized source. – A network problem exists.
Post-conditions	The parameter value(s) of the ETS feature for which modification was requested are updated.

6.4.4 Cancel modification of ETS parameters

Name	Cancel modification of ETS parameters
Summary	The SC that submitted an earlier request for ETS parameter modification (see 6.4.3) can cancel the request before the request is completed (as indicated by a completion notification issued by the SP).
Actor(s)	Service Customer (SC)
Assumptions	None
Pre-conditions	The SC has made an earlier request for ETS parameter modification. Completion of the earlier request has not yet occurred, i.e., the request is in the "open/active" state as defined by Annex A.
Begins when	SC decides to cancel the original request.
Description	SC issues a cancellation request prior to completion of the earlier ETS parameter modification request. If cancellation is successful, then SC is notified of success. If cancellation is unsuccessful, SC receives an exception report or confirmation that the original ETS parameter modification request was successful.

Ends when	SC receives a success notification, an exception report, or an ETS parameter modification confirmation.
Exceptions	– Original request has been completed (i.e., is in the "closed" state as defined by Annex A). – Too late to cancel. – The request originates from an unauthorized source.
Post-conditions	Original request is cancelled. A record of the original request and the cancellation may be kept available for future query (optional).

6.4.5 Request for deactivation of ETS features

Name	Request for deactivation of ETS features
Summary	In situations where ETS features are not always active, the SC can deactivate ETS features. The SP notifies the SC when the requested deactivation has occurred. In terms of ITU-T Rec. X.731, *State management function*, deactivation of an ETS feature changes the administrative state of the ETS feature from "unlocked" to "locked".
Actor(s)	Service Customer (SC)
Assumptions	See assumptions for the request for activation of ETS features use-case (see 6.4.1).
Pre-conditions	ETS features are in an "active" state (or "unlocked" per ITU-T Rec. X.731), e.g., a previous request for activation had been completed earlier (see 6.4.1).
Begins when	The SC requests deactivation of ETS features.
Description	When the SC issues a request for ETS feature deactivation, the SC will specify certain parameters as part of the request (e.g., identification of ETS feature(s) to be deactivated). Once the requested ETS feature(s) is deactivated, the SP notifies the SC that the deactivation is complete.
Ends when	The SP notifies the SC that the ETS feature(s) is deactivated.
Exceptions	– ETS feature was not previously activated. – SC cannot be properly authenticated.
Post-conditions	The ETS feature(s) is not in an activated state, i.e., in terms of ITU-T Rec. X.731, the administrative state of the ETS features is "locked".

6.4.6 Registration of authorized ETS user

Name	Registration of authorized ETS user
Summary	The SC registers with the SP a new authorized user (authorized to use one or more ETS features).
Actor(s)	Service Customer (SC)
Assumptions	The availability of emergency priority communication services is restricted to specifically authorized users supporting recovery operations. The SC generally does such registration in advance for those personnel identified as candidates for supporting emergency recovery operations. However, due to the unexpected occurrence and location of disaster situations there may be a requirement for real-time authorization, through a central coordination centre, of personnel needed immediately to support recovery operations. The SC can then pass the appropriate registration information to the SP so that timely authentication of valid users can be accomplished. The SC is responsible for determining whether or not a particular user is authorized. Once the SC registers an authorized user with the SP, the SP is responsible for authenticating this user at the time that the user attempts to access ETS features.
Pre-conditions	A pre-defined ETS service contract has been established and the SC has been pre-authorized to perform this function. Note that the SC may register users independently of whether or not ETS features have been activated (see 6.4.1).
Begins when	The SC requests registration of a new authorized user.
Description	When the SC issues a request to register a new authorized user, the SC will specify certain parameters as part of the request (e.g., friendly user name, unique userID, user PIN, ETS features that this authorization applies to, user priority level, etc.) When the user is registered, the SP notifies the SC that registration is complete.
Ends when	The SP notifies the SC that the new authorized ETS user has been registered.
Exceptions	– The user was previously registered. – The request originates from an unauthorized source. – Missing or incorrect parameter values. – Number of authorized users exceeded.
Post-conditions	New authorized ETS user is registered and a corresponding ETS user profile is maintained by the SP.

6.4.7 Modification of registered ETS user profile

Name	Modification of registered ETS user profile
Summary	The SC modifies the profile information for an authorized ETS user that has been registered with the SP.
Actor(s)	Service Customer (SC)
Assumptions	See assumptions for the registration of authorized ETS user use-case (see 6.4.6). Before requesting modification of a user profile, the SC may find it useful to "query" the user profile from the SP in order to verify the existing values of data items within the profile. It is assumed that this "query" will be supported even though it is not described via a separate use-case.
Pre-conditions	A registered ETS user profile exists with the SP, e.g., the registration of authorized ETS user had been completed earlier (see 6.4.6).
Begins when	The SC requests modification of a registered ETS user profile.
Description	When the SC issues a request to modify a registered ETS user profile, the SC will specify certain parameters as part of the request (e.g., unique userID, profile data items to be modified along with their new values, etc.). When the profile has been modified, the SP notifies the SC that the profile modification is complete.
Ends when	The SP notifies the SC that the requested profile modification has been completed.
Exceptions	– Missing or incorrect parameter values (i.e., profile data items). – User profile not found. – The request originates from an unauthorized source.
Post-conditions	The modified ETS user profile is maintained by the SP.

6.4.8 Deregistration of authorized ETS user

Name	Deregistration of authorized ETS user
Summary	An authorized ETS user that has been previously registered with the SP is deregistered by the SC.
Actor(s)	Service Customer (SC)
Assumptions	The population of authorized ETS users is dynamic and will change over time. This use-case allows deregistration of authorized ETS users. Clause 6.4.6 provides the use-case for registration of authorized ETS users.
Pre-conditions	A profile exists with the SP for the user to be deregistered, e.g., the registration of authorized ETS user had been completed earlier (see 6.4.6).
Begins when	The SC requests deregistration of an authorized ETS user.
Description	When the SC issues a request to deregister an authorized ETS user, the SC will specify certain parameters as part of the request (e.g., unique userID). When the ETS user is deregistered, the SP notifies the SC that deregistration is complete.
Ends when	The SP notifies the SC that the ETS user deregistration has been completed.
Exceptions	– User profile not found. – The request originates from an unauthorized source.
Post-conditions	The ETS user is deregistered and the corresponding profile is no longer maintained by the SP.

6.4.9 Requests for ETS status

Name	Requests for ETS status
Summary	The SC queries the SP to determine the operational state (defined in ITU-T Rec. X.731) of one or more ETS features.
Actor(s)	Service Customer (SC)
Assumptions	Anytime, the SC can request if specific ETS features are "available". The term "available" is used here to mean the network capability exists and is not experiencing a failure condition. Some ETS features may be active (i.e., in terms of ITU-T Rec. X.731, their administrative state is "unlocked"), but are not available because of limited network capacity. Other ETS features may only be activated upon specific request by the SC as indicated in 6.4.1. However, the SC could request the state of availability before the activation request is issued.
Pre-conditions	ETS network capabilities supporting ETS features are in place. Note that the ETS features may or may not be activated as defined in 6.4.1. A pre-defined ETS service contract has been established and the SC has been pre-authorized to perform this function.
Begins when	The SC sends a request for ETS status to the SP.
Description	When the SC sends a request for ETS status to the SP, the SC will specify certain parameters as part of the request (e.g., identification of the ETS feature(s) for which status is requested). The SP response to this query will include certain parameters (e.g., value of the operational state corresponding to each ETS feature for which status is requested, value of the administrative state corresponding to each ETS feature for which status is requested, etc.).
Ends when	SP response containing ETS status information is sent to SC.
Exceptions	– Invalid ETS feature identification. – The request originates from an unauthorized source.
Post-conditions	SC has received requested ETS status information.

6.4.10 Requests for specific on-demand reports about ETS

Name	Requests for specific on-demand reports about ETS
Summary	The SC requests that the SP start issuing one or more specific on-demand reports about ETS.
Actor(s)	Service Customer (SC)
Assumptions	The SC may request specific reports or specific sets of reports individually anytime. The SC may terminate the delivery of a report anytime as described in the stop during delivery of report use-case (see 6.4.11). Note that there is no size restriction on how large a report may be. Therefore, the SP may deliver the requested report to the SC in multiple parts. It is also possible for a report to have no defined ending (e.g., continuous report of data being monitored by the SP). This type of report would need to be stopped using the stop during delivery of report use-case (see 6.4.11).
Pre-conditions	A pre-defined ETS service contract has been established identifying what types of ETS reports may be requested by the SC. The SC has been pre-authorized to perform this function.

Begins when	SC sends a request to the SP to start issuing one or more specific on-demand reports about ETS.
Description	When the SC sends a request for on-demand reports about ETS to the SP, the SC will specify certain parameters as part of the request (e.g., type of report(s) for SP to send, etc.). The SP response to this request may occur in multiple parts. Each partial response notification will include certain parameters (e.g., identification of report type, report data, indication of whether or not this is the final part of the report, indication of how many more parts of the report will be coming subsequently, etc.).
Ends when	Final part of all reports requested has been sent to the SC by the SP, or when the stop during delivery of report use-case (see 6.4.11) occurs.
Exceptions	– Invalid report type requested. – The request originates from an unauthorized source.
Post-conditions	SC has received the on-demand reports about ETS that were requested, or has received partial report information up until the point that the stop during delivery of report use-case (see 6.4.11) occurred.

6.4.11 Stop during delivery of report

Name	Stop during delivery of report
Summary	The SC requests stoppage of on-demand reports about ETS that were previously started when the request for specific on-demand reports about ETS use-case occurred (see 6.4.10).
Actor(s)	Service Customer (SC)
Assumptions	See assumptions for the request for specific on-demand reports about ETS use-case (see 6.4.10).
Pre-conditions	The SC has previously started specific on-demand reports about ETS (see 6.4.10), and the final part of all reports requested has not yet been sent by the SP to the SC.
Begins when	SC sends a request to the SP to stop delivery of report(s) that have not yet been completed.
Description	When the SC sends a request to stop delivery of report(s) that have not yet been completed, the SC will specify certain parameters as part of the request (e.g., type of report(s) to stop, etc.). When the SP has stopped the specific report(s) for which stoppage was requested, the SP notifies the SC that the report stoppage has occurred.
Ends when	The SP notifies the SC that the report stoppage has occurred.
Exceptions	– On-demand report has already normally completed. – The request originates from an unauthorized source.
Post-conditions	No further parts of the stopped report(s) are sent to the SC.

6.4.12 Administration of alert triggers

Name	Administration of alert triggers
Summary	The SC administers (i.e., modifies) the trigger conditions that will cause an alert to be sent from the SP to the SC.
Actor(s)	Service Customer (SC)
Assumptions	Three alert types are defined in 6.4.15 through 6.4.17. The sending of an alert is triggered by some network event that is detected by the SP. This use-case allows the SC to administratively determine which network events will trigger the sending of an alert and which will not. This is accomplished by modifying the "alert trigger profile". Before requesting modification of the alert trigger profile, the SC may find it useful to "query" the alert trigger profile from the SP in order to verify the existing values of data items within the profile. It is assumed that this "query" will be supported even though it is not described via a separate use-case.
Pre-conditions	A pre-defined ETS service contract has been established identifying what types of alerts the SC may choose to receive and the set of triggers that the SC may select from to cause alerts to be sent. An alert trigger profile exists with the SP (e.g., set up by the SP with default values).
Begins when	The SC requests modification of the alert trigger profile.
Description	When the SC issues a request to modify the alert trigger profile, the SC will specify certain parameters as part of the request (e.g., alert type to be turned "on" or "off", profile data items/trigger conditions to be modified along with their new values, etc.). When the profile has been modified, the SP notifies the SC that the profile modification is complete.
Ends when	The SP notifies the SC that the requested profile modification has been completed.
Exceptions	– Missing or incorrect parameter values (i.e., profile data items). – Alert trigger profile not found. – Invalid trigger requested. – The request originates from an unauthorized source.
Post-conditions	The modified alert trigger profile is maintained by the SP.

6.4.13 Administration of scheduled reports

Name	Administration of scheduled reports
Summary	The SC administers (i.e., modifies) the trigger conditions (i.e., schedule) that will cause a scheduled report to be sent from the SP to the SC.
Actor(s)	Service Customer (SC)
Assumptions	One scheduled report type is defined in 6.4.18 (other scheduled report types may be defined in the future). "Scheduled reports" are reports that are to be provided by the SP and delivered on an agreed upon schedule. This use-case allows the parameters for the schedule to be administered through requests provided by the SC. This is accomplished by modifying the "reporting schedule". Before requesting modification of the reporting schedule, the SC may find it useful to "query" the reporting schedule from the SP in order to verify the existing values of data items within the schedule. It is assumed that this "query" will be supported even though it is not described via a separate use-case.

Pre-conditions	A pre-defined ETS service contract has been established identifying what types of reports the SC may choose to schedule and the set of parameters that the SC may select from in order to define the schedule. A reporting schedule exists with the SP (e.g., set up by the SP with default values).
Begins when	The SC requests modification of the reporting schedule.
Description	When the SC issues a request to modify the reporting schedule, the SC will specify certain parameters as part of the request (e.g., report type to be scheduled, data items to be modified along with their new values, etc.). When the reporting schedule has been modified, the SP notifies the SC that the schedule modification is complete.
Ends when	The SP notifies the SC that the requested schedule modification has been completed.
Exceptions	– Missing or incorrect parameter values (i.e., schedule data items). – Reporting schedule not found. – Invalid report type requested. – The request originates from an unauthorized source.
Post-conditions	The modified reporting schedule is maintained by the SP.

6.4.14 Submission of ETS trouble reports

ETSMS shall include the trouble management function for ITU-T applications as specified by ITU-T Rec. X.790. The following capabilities (as specified by ITU-T Rec. X.790) shall be available to the Service Customer:

- Trouble report creation;
- Tracking trouble reports;
- Management of trouble reports;
- Trouble report clearing and closure.

6.4.15 ETS status change alerts

Name	ETS status change alerts
Summary	The SP detects a change in the status (e.g., failure occurs) of ETS service and alerts the SC of this condition.
Actor(s)	Service Customer (SC)
Assumptions	SP reports on status of ETS service would be provided when the state of service status changes, and when there is a service failure. The reports could cover the overall status of service performance including types of service and areas of coverage.
Pre-conditions	A pre-defined ETS service contract has been established identifying what types of ETS service status information may be made available to the SC via ETS status change alerts. The SC has administratively requested to receive ETS status change alerts (e.g., via the administration of alert triggers use-case defined in 6.4.12).
Begins when	The SP detects a change in the status (e.g., failure occurs) of ETS service that may be made available to the SC.
Description	The SP issues an alert notification to the SC. The notification will include certain parameters (e.g., description of the ETS status change that occurred).
Ends when	The SC receives ETS status change alert.
Exceptions	None
Post-conditions	SC is informed of ETS status change.

6.4.16 ETS security event alerts

Name	ETS security event alerts
Summary	The SP detects a security-related event and alerts the SC of this condition.
Actor(s)	Service Customer (SC)
Assumptions	SP reports on security aspects when triggered by a specific event or change of status. The report could include identification of type of event, such as denial of service or attempted unauthorized access. The reports could include specific instances and locations of the security events. If ETS service is degraded due to the security-related event being reported, then ETS degradation alert may also be issued (see 6.4.17).
Pre-conditions	A pre-defined ETS service contract has been established identifying what types of ETS security event alerts may be made available to the SC. The SC has administratively requested to receive ETS security event alerts (e.g., via the administration of alert triggers use-case defined in 6.4.12).
Begins when	The SP detects a security-related event that may be made available to the SC.
Description	The SP issues an alert notification to the SC. The notification will include certain parameters (e.g., description of the security-related event detected, impact of the event on ETS service if known, etc.).
Ends when	The SC receives the ETS security event alert.
Exceptions	None
Post-conditions	SC is informed of the security-related event.

6.4.17 ETS degradation alerts

Name	ETS degradation alerts
Summary	The SP detects that one or more ETS Quality of Service (QoS) parameter values have degraded below the values specified in the SLA and alerts the SC of this condition.
Actor(s)	Service Customer (SC)
Assumptions	As SP resources become unavailable (e.g., due to SP network infrastructure and service failures, or due to SP network infrastructure security breaches, or due to heavy traffic), the ETS QoS that is normally expected for the specific mode of communication could progressively degrade below the values specified in the SLA. The ETS SLA may include a policy definition by which the SC and the SP agree that under such conditions the SP might automatically apply traffic controls in the network. Alternatively, the SP response might be to just put all ETS services on a best effort basis. However, traffic controls may be used in order to limit only the most bandwidth-demanding traffic (e.g., video broadcast) in order to preserve effective interchange of the most critical information in a message format. A graceful response could be progressive, starting with high bandwidth services, and continuing (if necessary) by selectively restricting the narrow-band command and control type of interchange. Flexibility is needed in the definition of the data elements to cover a range of possibilities.

Pre-conditions	A pre-defined ETS service contract (i.e., SLA) has been established with defined QoS parameters and values. The SC has administratively requested to receive ETS degradation alerts (e.g., via the administration of alert triggers use-case defined in 6.4.12).
Begins when	The SP detects that one or more ETS QoS parameter values have degraded below the values specified in the SLA.
Description	The SP issues an alert notification to the SC. The notification will include certain parameters (e.g., the current QoS parameter values that have been detected, any traffic controls that may have been put in effect by the SP in response to the degradation, etc.).
Ends when	The SC receives the ETS degradation alert.
Exceptions	None
Post-conditions	SC is informed of ETS QoS degradation and SP response to degradation (when applicable).

6.4.18 ETS usage reports

Name	ETS usage reports
Summary	The SP provides ETS usage reports to the SC on a periodic schedule.
Actor(s)	Service Customer (SC)
Assumptions	The SP reports on ETS service usage could include statistical information about the actual usage of different types of service and areas of coverage for analysis purposes. Usage data may be broken down by individual ETS user, by ETS feature, or by other categories meaningful to the SC. These reports would be provided on a periodic schedule.
Pre-conditions	A pre-defined ETS service contract has been established identifying what types of ETS usage reports may be made available to the SC. The SC has administratively set up a schedule to receive ETS usage reports identifying the types of reports to be sent and the schedule for issuing the reports, e.g., via the administration of scheduled reports use-case defined in 6.4.13.
Begins when	Date/time for issuing a report is reached (according to the schedule previously established by the SC).
Description	The SP sends an ETS usage report to the SC. The report notification will include certain parameters (e.g., identification of report, time sent, etc.).
Ends when	The SC receives the ETS usage report.
Exceptions	None
Post-conditions	SC is informed of ETS usage.

7 Interface requirements

Crisis situations that require immediate recovery operations to save lives, restore the community infrastructure, and bring the population back to normal living conditions can happen unexpectedly anyplace at anytime. Therefore, it is imperative that personnel deployed for recovery operations be able to utilize resources that are readily available and within convenient reach. Specialized operational resources will very likely not be at hand immediately to facilitate recovery operations. Establishment of interfaces between emergency operations SCs and the SP of public telecommunication resources that are widely and commonly available are highly desirable. Consideration needs to be given to the human interface to ensure that it is simple, but effective. For example, the use of a basic web browser could provide a commonly and easily used means of fulfilling the requirements for interchange of critical service management information between disaster relief operations SCs and telecommunication SPs as described in clause 6. The specification for the interface requirements is a subject of other ITU-T Recommendations.

Another critical factor for establishing an efficient and effective interface for interchange of service and network management information between TMNs across the X-interface is standardization of data elements that represent appropriate information associated with emergency recovery operations. Standardized data elements for management information interchange need to be identified for application to disaster relief operations. In addition, specialized data elements may need to be defined and standardized that would apply uniquely to emergency recovery operations. The definition of the appropriate data elements for emergency communications will be specified by other ITU-T Recommendations.

Annex A

ETS request state model

This Annex describes an ETS request state model applicable to the following use-cases:

- Cancel modification of ETS parameters (see 6.4.4)
- Cancel request for activation of ETS features (see 6.4.2)
- Modification of ETS parameters (see 6.4.3)
- Request for activation of ETS features (see 6.4.1).

The ETS request state model is based on (and simplified from) the request state model found in ITU-T Rec. M.3208.1.

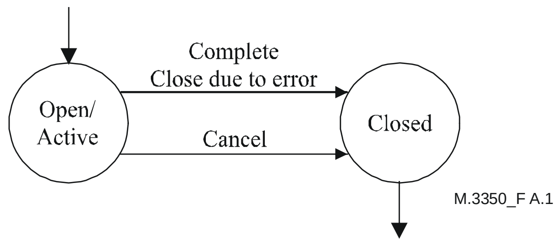


Figure A.1/M.3350 – Request state model

Table A.1/M.3350 – State transition table for request state model

Event	Current state	
	Open/Active	Closed
complete	service request completed ⇒ closed	
error	emit error event ⇒ closed	
cancel	closed	

NOTE – All requests (Modification of ETS parameters, Request for activation of ETS features) begin in the "Open/Active" state.

Signalling Systems

Signalling for IEPS support in ISUP

Q.761 Amendment 3

Q.762 Amendment 3

Q.763 Amendment 4

Q.764 Amendment 4

ITU-T Rec. Q.761 Amendment 3 (01/2006)

SIGNALLING SYSTEM NO. 7 – ISDN USER PART FUNCTIONAL DESCRIPTION: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) for disaster recovery operations as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.761 (1999) in order to accommodate these needs. This amendment should be read in conjunction with Amendment 3 to ITU-T Rec. Q.762, Amendment 4 to ITU-T Rec. Q.763, and Amendment 4 to ITU-T Rec. Q.764. This amendment incorporates Amendment 2 to ITU-T Rec. Q.761 and provides enhancements.

1) Clause 1.1 – Scope

Insert the following paragraph at the end of this clause (below the Note):

The International Emergency Preference Scheme is described in ITU-T Rec. E.106, *International Emergency Preference Scheme (IEPS) for Disaster Relief Operations* [12]. The associated ISUP functional descriptions, formats and codes, and procedures are to be found in ITU-T Recs Q.762 [6], Q.763 [7], and Q.764 [8].

2) Clause 1.2 – References

Add the following new references:

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

[13] ITU-T Recommendation E.412 (2003), *Network management controls*.

[14] ITU-T Recommendation Q.767 (1991), *Application of the ISDN User Part of CCITT signalling system No. 7 for international ISDN interconnections*.

[15] ITU-T Recommendation Q.1902.x series (2001), *Bearer Independent Call Control protocol (Capability Set 2)*.

3) Clause 1.3 – Terms and definitions

Add the following new definitions:

1.3.6 ISUP'97: 1997 release of ISUP Recommendations.

1.3.7 ISUP 2000: 1999 release of ISUP Recommendations.

4) Clause 2.4.1 – ISUP Interworking

Insert the appropriate reference number [14] after each appearance of ITU-T Rec. Q.767.

5) Clause 3 – Capabilities supported by the ISDN user part

Insert the following new entry and Note into Table 1/Q.761:

Table 1/Q.761

Function/service	National use	International
International Emergency Preference Scheme	√ (Note)	√
NOTE – The procedures specified here for the international signalling network can be applied in national networks also. It is essential that the call is set up in the originating and destination national networks with utmost priority.		

6) New Appendix II

Insert the following new Appendix II:

Appendix II/Q.761

ISUP enhancements to support IEPS

II.1 Introduction

There is an urgent need for enhancements to ISUP implementations in support of the International Emergency Preference Scheme (IEPS) as specified in ITU-T Rec. E.106 [12]. The intent is to increase the probability of call completion in congested network situations for authorized callers. These enhancements only apply to the international interface. Administrations and network operators are encouraged to support these or similar capabilities in their domestic networks.

II.2 Scope

This appendix provides an overview of the signalling needed to support IEPS. The ISUP enhancements to the other ITU-T Recommendations of this series relating to basic call are provided in corresponding amendments to ITU-T Recs Q.762, Q.763, and Q.764. To provide a viable IEPS capability, it is required to implement all the amendments to the ITU-T Recommendations of this series.

II.3 Approach

The implementation of IEPS support may take place in a phased approach in a forward compatible manner. This phased approach facilitates and expedites the introduction of IEPS and allows its support by different ISUP versions. The phases are:

a) The minimum implementation relies on the transfer in ISUP of a specific IEPS call marking in the forward direction for preferential call set-up in the international network. In an international exchange, any call attempt with this IEPS call marking shall bypass restrictive call handling procedures (for example network management controls as specified in ITU-T Rec. E.412 [13]).

b) An improved implementation provides the generation of an early ACM. The aim of this mechanism is to reduce call set-up failures due to timer expiration caused by, for example, queuing delays for trunk allocation on congested routes.

c) An additional information transfer mechanism, based on a new parameter in conjunction with the IEPS call marking, is used to facilitate enhancements of IEPS in the areas of identification and priority levels.

II.4 ISUP versions and ISUP-based protocols

As the ISUP'2000 specifications [6], [7], [8] are published in different ITU-T Recommendations, these amendments to ISUP provide all necessary information for support of IEPS in international exchanges. IEPS can be implemented on the previous versions ISUP'92 and ISUP'97 by the identical amendments made for ISUP'2000. In support of IEPS, ITU-T Recs Q.767 [14] and Q.1902.x series [15] are also being amended.

ITU-T Rec. Q.762 Amendment 3 (01/2006)

SIGNALLING SYSTEM NO. 7 – ISDN USER PART GENERAL FUNCTIONS OF MESSAGES AND SIGNALS: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) for disaster recovery operations as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.762 (1999) in order to accommodate these needs. This amendment should be read in conjunction with Amendment 3 to ITU-T Rec. Q.761, Amendment 4 to ITU-T Rec. Q.763, and Amendment 4 to ITU-T Rec. Q.764. This amendment incorporates Amendment 1 to ITU-T Rec. Q.762 and provides enhancements.

1) Clause 1.4 – Abbreviations

Insert the following new abbreviation alphabetically:

IEPS International Emergency Preference Scheme

2) Clause 3 – Signalling parameters

Add the following new definition to clause 3:

3.102 IEPS call information: Information sent in the forward direction to convey IEPS call-related information.

3) Clause 4 – Parameter information

Add the following new definitions to clause 4:

4.161 country/international network of call origination: Information sent in the forward direction identifying the country or the international network of IEPS call origination.

4.162 priority level: Information sent in the forward direction that indicates national priority level of an IEPS call.

ITU-T Rec. Q.763 Amendment 4 (01/2006)

SIGNALLING SYSTEM NO. 7 – ISDN USER PART FORMATS AND CODES: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) for disaster recovery operations as specified in ITU-T Rec. E.106. This amendment contains the modifications to ITU-T Rec. Q.763 (1999) in order to accommodate these needs. It should be read in conjunction with Amendment 3 to ITU-T Rec. Q.761, Amendment 3 to ITU-T Rec. Q.762, and Amendment 4 to ITU-T Rec. Q.764. This amendment incorporates Amendment 2 to ITU-T Rec. Q.763 and provides enhancements.

1) Clause 0.4 – Abbreviations

Insert the following new abbreviation alphabetically:

IEPS International Emergency Preference Scheme

2) Clause 3.11 – Calling party's category

Change the following in Figure 12, which had been a spare value:

0 0 0 0 1 1 1 0 ~~spare~~IEPS call marking for preferential call set up

3) Table 5

Modify Table 5 in order to introduce the following new IEPS call information parameter (3.103) alphabetically:

Table 5/Q.763

Parameter name	Reference (subclause)	Code
IEPS call information	3.103	1 0 1 0 0 1 1 0

4) New clause 3.103 – IEPS call information

Add new clause 3.103 as follows:

3.103 IEPS call information

The format of the IEPS call information parameter field is shown in Figure 96-a.

	8	7	6	5	4	3	2	1
1	Country/International network of call origination							
2	Priority level							

Figure 96-a/Q.763 – IEPS call information parameter field

The following codes are used in the subfields of the IEPS call information parameter field:

a) Country/International network of call origination

<table>
<tr><td></td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>1</td><td>O/E</td><td>spare</td><td colspan="3">Numbering plan indicator</td><td colspan="3">Length of country/international network of call origination</td></tr>
<tr><td>1a</td><td colspan="4">2nd digit</td><td colspan="4">1st digit</td></tr>
<tr><td>1b</td><td colspan="4"></td><td colspan="4"></td></tr>
<tr><td></td><td colspan="4"></td><td colspan="4"></td></tr>
<tr><td>1m</td><td colspan="4">Filler (if necessary)</td><td colspan="4">Nth digit</td></tr>
</table>

Figure 96-b/Q.763 – Country/International network of call origination subfield

1) *Odd/even indicator (O/E):* as in 3.9 a).

2) *Numbering plan indicator*

000 spare

001 numbering plan according to ITU-T Rec. X.121

010 numbering plan according to ITU-T Rec. E.164

3) *Length of country/international network of call origination*

Number of octets to follow that contain the digits identifying the country or international network of call origination.

4) *Digits*

Digit string of flexible length in BCD encoding identifying either the country or international network of call origination. To identify a specific country of call origination, the digit string will consist of the X.121 country code (3 digits). To identify an international network of call origination, the digit string will consist of an E.164 country code for international networks (3 digits) followed by an identification code (1 to 4 digits) to identify the international network.

5) *Filler*

In case of an odd number of digits, the filler code 0000 is inserted after the last digit.

b) Priority level

<table>
<tr><td></td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>2</td><td colspan="3">spare</td><td colspan="5">Priority level</td></tr>
</table>

Figure 96-c/Q.763 – Priority level subfield

This subfield carries national priority level of an IEPS call according to bilateral agreements. The priority level is signalled in inverse order of the numerical value. i.e., the lower the numerical value is, the higher the priority. For example, numerical value 0 indicates the highest priority possible.

5) Table 32

Add new IEPS call information parameter prior to the "End of optional parameters":

Table 32/Q.763

Message Type: Initial address

Parameter	Reference (subclause)	Type	Length (octets)
IEPS call information	3.103	O	6-8

ITU-T Rec. Q.764 Amendment 4 (01/2006)

SIGNALLING SYSTEM NO. 7 – ISDN USER PART SIGNALLING PROCEDURES: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) for disaster recovery operations as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.764 (1999) in order to accommodate these needs. This amendment should be read in conjunction with Amendment 3 to ITU-T Rec. Q.761, Amendment 3 to ITU-T Rec. Q.762, and Amendment 4 to ITU-T Rec. Q.763. This amendment incorporates Amendment 2 to ITU-T Rec. Q.764 and provides enhancements.

1) Clause 1.2 – References

Insert the following new reference:

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

2) Clause 1.4 – Abbreviations

Add the following new abbreviations alphabetically:

CPC Calling Party's Category

IEPS International Emergency Preference Scheme

3) Clause 2.1.1.3 – Actions required at an outgoing international exchange

Add the following:

e) *International Emergency Preference Scheme*

If an outgoing international exchange receives information from the national network that the call is to be treated as an IEPS call (e.g., CPC value of IEPS), call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, ISUP Signalling Congestion Control, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

If routing procedures fail to find an outgoing circuit, the call is queued and shall take precedence over any other normal call attempts.

Optionally, if queuing occurs, an early ACM (called party status set to "no indication") with the inclusion of the generic notification parameter set to "call completion delay" may be returned to the originating exchange. However, if the incoming IAM had requested continuity check (either on this circuit or a previous circuit), the early ACM (no indication) shall not be sent until a successful continuity indication has been received.

4) Clause 2.1.1.4 – Actions required at an intermediate international exchange

Add the following:

e) *International Emergency Preference Scheme*

If an intermediate international exchange receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, ISUP Signalling Congestion Control, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

If routing procedures fail to find an outgoing circuit, the call is queued and shall take precedence over any other normal call attempts.

Optionally, if queuing occurs, an early ACM (called party status set to "no indication") with the inclusion of the generic notification parameter set to "call completion delay" may be returned to the originating exchange. However, if the incoming IAM had requested continuity check (either on this circuit or a previous circuit), the early ACM (no indication) shall not be sent until a successful continuity indication has been received.

5) Clause 2.1.1.5 – Actions required at an incoming international exchange

Add the following:

e) *International Emergency Preference Scheme*

If an incoming international exchange receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking or national specific information for IEPS call treatment in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, ISUP Signalling Congestion Control, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

If routing procedures fail to find an outgoing circuit, the call is queued and shall take precedence over any other normal call attempts.

Optionally, if queuing occurs, an early ACM (called party status set to "no indication") with the inclusion of the generic notification parameter set to "call completion delay" may be returned to the originating exchange. However, if the incoming IAM had requested continuity check (either on this circuit or a previous circuit), the early ACM (no indication) shall not be sent until a successful continuity indication has been received.

6) Clause 2.1.2.3 – Actions required at an outgoing international exchange

Add the following:

e) *International Emergency Preference Scheme*

If an outgoing international exchange receives information from the national network that the call is to be treated as an IEPS call (e.g., CPC value of IEPS), call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, ISUP Signalling Congestion Control, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

If routing procedures fail to find an outgoing circuit, the call is queued and shall take precedence over any other normal call attempts.

Optionally, if queuing occurs, an early ACM (called party status set to "no indication") with the inclusion of the generic notification parameter set to "call completion delay" may be returned to the originating exchange. However, if the incoming IAM had requested continuity check (either on this circuit or a previous circuit), the early ACM (no indication) shall not be sent until a successful continuity indication has been received.

7) Clause 2.1.2.4 – Actions required at an intermediate international exchange

Add the following:

e) *International Emergency Preference Scheme*

If an intermediate international exchange receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, ISUP Signalling Congestion Control, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

If routing procedures fail to find an outgoing circuit, the call is queued and shall take precedence over any other normal call attempts.

Optionally, if queuing occurs, an early ACM (called party status set to "no indication") with the inclusion of the generic notification parameter set to "call completion delay" may be returned to the originating exchange. However, if the incoming IAM had requested continuity check (either on this circuit or a previous circuit), the early ACM (no indication) shall not be sent until a successful continuity indication has been received.

8) Clause 2.1.2.5 – Actions required at an incoming international exchange

Add the following:

e) *International Emergency Preference Scheme*

If an incoming international exchange receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking or national specific information for IEPS call treatment in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, ISUP Signalling Congestion Control, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

If routing procedures fail to find an outgoing circuit, the call is queued and shall take precedence over any other normal call attempts.

Optionally, if queuing occurs, an early ACM (called party status set to "no indication") with the inclusion of the generic notification parameter set to "call completion delay" may be returned to the originating exchange. However, if the incoming IAM had requested continuity check (either on this circuit or a previous circuit), the early ACM (no indication) shall not be sent until a successful continuity indication has been received.

9) New clause 2.28

Add the following new clause:

2.28 IEPS call information

2.28.1 Actions required at an outgoing international gateway exchange

Where the exchange logic determines that an IEPS call (as set out in 2.1.1.3 e and 2.1.2.3 e) requires IEPS information to be transported in the forward direction and based on bilateral agreement between administrations, the exchange shall include the IEPS call information parameter in the outgoing IAM. This parameter will contain the identity of the entity (the country or international network) originating the IEPS call, and the national priority level of the call. The priority level in the IEPS call information parameter will be the national priority level of the call in the entity originating the call. The priority level in the IEPS call information parameter is signalled in inverse order of the numerical value, i.e., the lower the numerical value is, the higher the priority. For example, numerical value 0 indicates the highest priority possible.

2.28.2 Actions required at an intermediate international exchange

If an intermediate international exchange receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS in the outgoing IAM. The IEPS call information parameter shall be passed on transparently. The exchange shall not provide IEPS priority treatment if the CPC value is not IEPS, even if the optional IEPS call information parameter is present.

2.28.3 Actions required at an incoming international gateway exchange

If an incoming international gateway exchange receives a call with CPC set to IEPS, the call establishment proceeds with priority. On receipt of the IEPS call information parameter, the incoming international gateway exchange may provide enhanced service features by analysing the contents of this parameter. The exchange may provide a mapping of the IEPS priority level received from the entity (the country or international network) originating the IEPS call to that of the entity (the country or international network) of call destination. In case mapping is not implemented, the IEPS call information parameter may be discarded, however, the call shall continue to be treated as a priority call. The call is established with the CPC set as IEPS or national specific information for IEPS call treatment in the outgoing IAM.

If the IEPS call information parameter is expected (due to bilateral agreements) but is not received for an IEPS call (i.e., CPC is set to IEPS), the call establishment proceeds with priority. If the IEPS call information parameter is received containing a value (country/international network code and/or priority level), which has not been bilaterally agreed for an IEPS call (i.e., CPC is set to IEPS), the call establishment proceeds with priority. The call is established with the CPC set as IEPS or national specific information for IEPS call treatment in the outgoing IAM. A default priority value will be used for the call in the entity of call destination. The exchange shall not provide IEPS priority treatment if the CPC value is not IEPS, even if the optional IEPS call information parameter is present.

Signalling for IEPS support in BICC

Q.1902.1 Amendment 2

Q.1902.2 Amendment 3

Q.1902.3 Amendment 3

Q.1902.4 Amendment 3

ITU-T Rec. Q.1902.1 Amendment 2 (01/2006)

BEARER INDEPENDENT CALL CONTROL PROTOCOL (CAPABILITY SET 2): FUNCTIONAL DESCRIPTION: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) for disaster recovery operations as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.1902.1 (2001) in order to accommodate these needs. This amendment should be read in conjunction with Amendment 3 to ITU-T Rec. Q.1902.2, Amendment 3 to ITU-T Rec. Q.1902.3, and Amendment 3 to ITU-T Rec. Q.1902.4. This amendment incorporates Amendment 1 to ITU-T Rec. Q.1902.1 and provides enhancements.

1) Clause 1 – Scope

Insert the following paragraph at the end of this clause:

The International Emergency Preference Scheme is described in ITU-T Rec. E.106, International Emergency Preference Scheme (IEPS) for Disaster Relief Operations [64]. The associated BICC general functions of messages and parameters, formats and codes, and procedures are to be found in ITU-T Recs Q.1902.2 [14], Q.1902.3 [15], Q.1902.4 [16] and Q.1950 [61].

2) Clause 2 – References

Add the following new references:

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

[65] ITU-T Recommendation Q.767 (1991), *Application of the ISDN User Part of CCITT signalling system No. 7 for international ISDN interconnections*.

3) Clause 3 – Definitions

Insert the following new terms alphabetically and renumber the subsequent terms accordingly:

3.13 ISUP'92: 1993 publication of ISUP Recommendations.

3.14 ISUP'97: 1997 publication of ISUP Recommendations.

3.15 ISUP'2000: 1999 publication of ISUP Recommendations.

4) Clause 8 – Capabilities supported

Insert the following new entry into Table 1/Q.1902.1:

Table 1/Q.1902.1 – Signalling capabilities for basic call

Function/service	National use	International
International Emergency Preference Scheme	√ (Note 4)	√
NOTE 4 – The procedures specified here for the international signalling network can be applied in national networks also. It is essential that the call is set up in the originating and destination national networks with utmost priority.		

5) New Appendix II

Insert the following new Appendix II:

Appendix II/Q.1902.1

BICC enhancements to support IEPS

II.1 Introduction

There is an urgent need for enhancements to BICC implementations in support of the International Emergency Preference Scheme (IEPS) as specified in ITU-T Rec. E.106 [64]. The intent is to increase the probability of call completion in congested network situations for authorized callers. These enhancements only apply to the international interface. Administrations, and network operators are encouraged to support these, or similar capabilities, in their domestic networks.

II.2 Scope

This appendix provides an overview of the signalling needed to support IEPS. The BICC enhancements to the other ITU-T Recommendations of this series relating to basic call are provided in corresponding amendments to ITU-T Recs Q.1902.2, Q.1902.3, and Q.1902.4. To provide a viable IEPS capability, it is required to implement all the amendments to the ITU-T Recommendations of this series.

II.3 Approach

The implementation of IEPS support may take place in a phased approach in a forward compatible manner. This phased approach facilitates and expedites the introduction of IEPS. The phases are:

a) The minimum implementation relies on the transfer in BICC of a specific IEPS call marking in the forward direction for preferential call set-up in the international network. In an international exchange, any call attempt with this IEPS call marking shall bypass restrictive call handling procedures (for example, network management controls as specified in ITU-T Rec. E.412 [35]).

b) An improved implementation provides the generation of an early ACM. The aim of this mechanism is to reduce call set-up failures due to timer expiration caused by, for example, queuing delays for trunk allocation on congested routes.

c) An additional information transfer mechanism, based on a new parameter in conjunction with the IEPS call marking, is used to facilitate enhancements of IEPS in the areas of identification and priority levels.

II.4 BICC versions and ISUP protocols

As the BICC CS-2 specifications ([14], [15], [16] and [61]) are published in different ITU-T Recommendations, these amendments to BICC provide all necessary information for support of IEPS in international exchanges. The support of IEPS by BICC CS-1 [13] is covered by the amendments to the ISUP'2000 series of Recommendations [6], [7], [8] and [9].

ITU-T Rec. Q.767 [65] and the ISUP'2000 series of Recommendations [6], [7], [8] and [9] are also being amended in support of IEPS. IEPS can be implemented on the previous versions ISUP'92 and ISUP'97 by the identical amendments made for the ISUP'2000 series of Recommendations.

ITU-T Rec. Q.1902.2 Amendment 3 (01/2006)

BEARER INDEPENDENT CALL CONTROL PROTOCOL (CAPABILITY SET 2) AND SIGNALLING SYSTEM NO. 7 ISDN USER PART: GENERAL FUNCTIONS OF MESSAGES AND PARAMETERS: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) for disaster recovery operations as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.1902.2 (2001) in order to accommodate these needs. This amendment should be read in conjunction with Amendment 2 to ITU-T Rec. Q.1902.1, Amendment 3 to ITU-T Rec. Q.1902.3, and Amendment 3 to ITU-T Rec. Q.1902.4. This amendment incorporates Amendment 1 to ITU-T Rec. Q.1902.2 and provides enhancements.

1) Clause 4 – Abbreviations

Insert the following new abbreviation alphabetically:

IEPS International Emergency Preference Scheme

2) Clause 6 – Signalling parameters

Insert new following definition alphabetically and renumber all subsequent subclauses accordingly:

IEPS call information: Information sent in the forward direction to convey IEPS call-related information.

3) Clause 7 – Parameter information

Insert new following definitions alphabetically and renumber all subsequent subclauses accordingly:

country/international network of call origination: Information sent in the forward direction identifying the country or the international network of IEPS call origination.

priority level: Information sent in the forward direction that indicates national priority level of an IEPS call.

ITU-T Rec. Q.1902.3 Amendment 3 (01/2006)

BEARER INDEPENDENT CALL CONTROL PROTOCOL (CAPABILITY SET 2) AND SIGNALLING SYSTEM NO. 7 ISDN USER PART: FORMATS AND CODES: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCES SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) for disaster recovery operations as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.1902.3 (2001) in order to accommodate these needs. This amendment should be read in conjunction with Amendment 2 to ITU-T Rec. Q.1902.1, Amendment 3 to ITU-T Rec. Q.1902.2, and Amendment 3 to ITU-T Rec. Q.1902.4. This amendment incorporates Amendment 1 to ITU-T Rec. Q.1902.3 and provides enhancements.

1) Clause 4 – Abbreviations

Add the following new abbreviation alphabetically:

IEPS International Emergency Preference Scheme

2) Clause 6.21 – Calling party's category

Change the following in Figure 39, which had been a spare value:

0 0 0 0 1 1 1 0 IEPS call marking for preferential call set-up

3) Table 2

Modify Table 2 in order to introduce the following new IEPS call information parameter (6.108) after "automatic re-routing":

Table 2/Q.1902.3 – Parameter name codes

Parameter name	Reference (clause)	Code	Note
IEPS call information	6.108	1010 0110	

4) New clause 6.108 – IEPS call information

Add new clause 6.108 as follows:

6.108 IEPS call information

The format of the IEPS call information parameter field is shown in Figure 125a.

	8	7	6	5	4	3	2	1
1	Country/International network of call origination							
2	Priority level							

Figure 125a/Q.1902.3 – IEPS call information parameter field

The following codes are used in the subfields of the IEPS call information parameter field:

a) Country/international network of call origination

	8	7	6	5	4	3	2	1
1	O/E	Spare	Numbering plan indicator			Length of country/international network of call origination		
1a	2nd digit				1st digit			
1b								
1m	Filler (if necessary)				Nth digit			

Figure 125b/Q.1902.3 – Country/international network of call origination subfield

1) *Odd/even indicator (O/E): as 6.17a) of Q.1902.3.*

2) *Numbering plan indicator*

   000 spare

   001 numbering plan according to ITU-T Rec. X.121

   010 numbering plan according to ITU-T Rec. E.164

3) *Length of country/international network of call origination*

   Number of octets to follow that contain the digits identifying the country or international network of call origination.

4) *Digits*

   Digit string of flexible length in BCD encoding identifying either the country or international network of call origination. To identify a specific country of call origination, the digit string will consist of the X.121 country code (3 digits). To identify an international network of call origination, the digit string will consist of an E.164 country code for international networks (3 digits) followed by an identification code (1 to 4 digits) to identify the international network.

5) *Filler*

   In case of an odd number of digits, the filler code 0000 is inserted after the last digit.

b) Priority level

	8	7	6	5	4	3	2	1
2	Spare			Priority level				

Figure 125c/Q.1902.3 – Priority level subfield

This subfield carries national priority level of an IEPS call according to bilateral agreements. The priority level is signalled in inverse order of the numerical value. i.e., the lower the numerical value is, the higher the priority. For example, numerical value 0 indicates the highest priority possible.

5) Table 38

Add new IEPS call information parameter between "Hop counter" and "IN service compatibility":

Table 38/Q.1902.3

Message Type: Initial address			
Parameter	**Reference (clause)**	**Type**	**Length (octets)**
IEPS call information	6.108	O	6-8

ITU-T Rec. Q.1902.4 Amendment 3 (01/2006)

BEARER INDEPENDENT CALL CONTROL PROTOCOL (CAPABILITY SET 2): BASIC CALL PROCEDURES: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCES SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) for disaster recovery operations as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.1902.4 (2001) in order to accommodate these needs. This amendment should be read in conjunction with Amendment 2 to ITU-T Rec. Q.1902.1, Amendment 3 to ITU-T Rec. Q.1902.2, and Amendment 3 to ITU-T Rec. Q.1902.3. This amendment incorporates Amendment 1 to ITU-T Rec. Q.1902.4 and provides enhancements.

1) Clause 4 – Abbreviations

Add the following new abbreviations alphabetically:

CPC Calling Party's Category

IEPS International Emergency Preference Scheme

2) Clause 7.2.2.3 – Actions required at an intermediate international SN

Add the following:

b) International Emergency Preference Scheme:

   i) If the CSF, at an intermediate international SN, receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

   ii) For an IEPS-call, the codec negotiation procedures are not to be invoked. If codec negotiation is already invoked on a preceding bearer path, the SN shall terminate the codec negotiation procedures and the call shall proceed.

   iii) If routing procedures fail to find an outgoing CIC value, the call is queued and shall take precedence over any other normal call attempts.

   iv) Optionally, if queuing occurs, an early ACM (called party status set to "*no indication*") with the inclusion of the generic notification parameter set to "*call completion delay*" may be returned to the preceding CSF. However, if the incoming IAM had indicated "*COT to be expected*", the early ACM (no indication) shall not be sent until Continuity Message (COT) with Continuity Indication has been received.

3) Clause 7.2.3.3 – Actions required at an intermediate international CMN

Add the following:

b) International Emergency Preference Scheme:

i) If the CSF, at an intermediate international CMN, receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

ii) If routing procedures fail to find an outgoing CIC value, the call is queued and shall take precedence over any other normal call attempts.

iii) Optionally, if queuing occurs, an early ACM (called party status set to "no indication") with the inclusion of the generic notification parameter set to "call completion delay" may be returned to the preceding CSF. However, if the incoming IAM had indicated "COT to be expected", the early ACM (no indication) shall not be sent until Continuity Message (COT) with Continuity Indication has been received.

4) Clause 7.2.4.3 – Actions required at an outgoing international gateway SN

Add the following:

c) International Emergency Preference Scheme:

i) If the CSF, at an outgoing international gateway SN, receives information from the national network that the call is to be treated as an IEPS call (e.g., CPC value of IEPS), call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

ii) For an IEPS-call, the codec negotiation procedures are not to be invoked. If codec negotiation is already invoked on a preceding bearer path, the SN shall terminate the codec negotiation procedures and the call shall proceed.

iii) If routing procedures fail to find an outgoing CIC value, the call is queued and shall take precedence over any other normal call attempts.

iv) Optionally, if queuing occurs, an early ACM (called party status set to "*no indication*") with the inclusion of the generic notification parameter set to "*call completion delay*" may be returned to the preceding CSF. However, if the incoming IAM had indicated "*COT to be expected*", the early ACM (no indication) shall not be sent until Continuity Message (COT) with Continuity Indication has been received.

5) Clause 7.2.5.3 – Actions required at an outgoing international gateway CMN

Add the following:

b) International Emergency Preference Scheme:

i) If the CSF, at an outgoing international gateway CMN, receives information from the national network that the call is to be treated as an IEPS call (e.g., CPC value of IEPS), call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

ii) If routing procedures fail to find an outgoing CIC value, the call is queued and shall take precedence over any other normal call attempts.

iii) Optionally, if queuing occurs, an early ACM (called party status set to "*no indication*") with the inclusion of the generic notification parameter set to "*call completion delay*" may be returned to the preceding CSF. However, if the incoming IAM had indicated "*COT to be expected*", the early ACM (no indication) shall not be sent until Continuity Message (COT) with Continuity Indication has been received.

6) Clause 7.2.6.3 – Actions required at an incoming international gateway SN

Add the following (after the Note):

a) International Emergency Preference Scheme:

i) If the CSF, at an incoming international gateway SN, receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking or national specific information for IEPS call treatment in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

ii) For an IEPS-call, the codec negotiation procedures are not to be invoked. If codec negotiation is already invoked on a preceding bearer path, the SN shall terminate the codec negotiation procedures and the call shall proceed.

iii) If routing procedures fail to find an outgoing CIC value, the call is queued and shall take precedence over any other normal call attempts.

iv) Optionally, if queuing occurs, an early ACM (called party status set to "*no indication*") with the inclusion of the generic notification parameter set to "*call completion delay*" may be returned to the preceding CSF. However, if the incoming IAM had indicated "*COT to be expected*", the early ACM (no indication) shall not be sent until Continuity Message (COT) with Continuity Indication has been received.

7) Clause 7.2.7.3 – Actions required at an incoming international gateway CMN

Add the following (after the Note):

a) International Emergency Preference Scheme:

   i) If the CSF, at an incoming international gateway CMN, receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS call marking or national specific information for IEPS call treatment in the outgoing IAM. Restrictive network management controls (e.g., Automatic Call Gapping, Automatic Congestion Control, Hard-to-Reach procedure) are not applied to this call.

   ii) If routing procedures fail to find a outgoing CIC value, the call is queued and shall take precedence over any other normal call attempts.

   iii) Optionally, if queuing occurs, an early ACM (called party status set to "no indication") with the inclusion of the generic notification parameter set to "call completion delay" may be returned to the preceding CSF. However, if the incoming IAM had indicated "COT to be expected", the early ACM (no indication) shall not be sent until Continuity Message (COT) with Continuity Indication has been received.

8) Clause 7.4 – Outgoing bearer set-up procedure

Add the following new paragraph and note at the end:

The BCF shall select appropriate bearer resources for a call with CPC set to IEPS to ensure that the quality of the bearer path is guaranteed throughout the lifetime of the call. This applies both to the set-up phase of the call as well as to the connection phase of the call in case of congested network situations. The CSF shall accordingly pass the IEPS indicator to the BCF in the BNC Information Request primitive and/or in the Bearer Set-up Request primitive.

NOTE – The emergency call indicator in Annex F/Q.1950 should no longer be used for IEPS.

9) Clause 7.5 – Incoming bearer set-up procedure

Add the following new paragraph and note at the end:

The BCF shall select appropriate bearer resources for a call with CPC set to IEPS to ensure that the quality of the bearer path is guaranteed throughout the lifetime of the call. This applies both to the set-up phase of the call as well as to the connection phase of the call in case of congested network situations. The CSF shall accordingly pass the IEPS indicator to the BCF in the BNC Information Request primitive and/or in the Bearer Set-up Request primitive.

NOTE – The emergency call indicator in Annex F/Q.1950 should no longer be used for IEPS.

10) New clause 7.4.6 Polling at an international SN for IEPS calls

Add new clause 7.4.6 as follows:

7.4.6 Polling at an international SN for IEPS calls

For IEPS calls at an international SN, for the above cases 7.4.1 to 7.4.5 where the BCF has indicated a failure due to temporary resource unavailability to the Bearer Set-up Request, or there has been no reply to the Bearer Set-up Request, the following optional polling procedure is initiated in the CSF:

1) An ACM (no indication) with the inclusion of the generic notification parameter set to "*call completion delay*" is returned to the incoming side. If the IAM indicated "*COT to be expected*" then the sending of the ACM (no indication) is delayed until the COT has been received. A polling guard timer (T44) is started to prevent the CSF to be polling an IEPS call for an excessive time.
2) The CSF may immediately send a Bearer Set-up Request to a different BCF for the purpose of selecting a different BIWF. If the BCF indicates a failure due to temporary resource unavailability to the Bearer Set-up Request, or there has been no reply to the Bearer Set-up Request, this step may be repeated towards other BCFs.
3) If Bearer Set-up Failure due to temporary resource unavailability is indicated, or there is no reply to the Bearer Set-up Request, by all BCFs in step 2 the CSF shall start a polling timer (T45).
4) On expiry of T45, the CSF shall send a Bearer Set-up Request to the first BCF. If Bearer Set-up Failure due to temporary resource unavailability is indicated, or there is no reply to the Bearer Set-up Request, steps 2 and 3 are repeated until a BCF indicates that resources are available. The time between successive polling attempts (T45) should be increased for each execution of step 3.

If the CSF receives a reply to the initial Bearer Set-up Request indicating "*Transaction Pending*", step 1 is executed and no further action is taken until the BCF responds further. If a BCF responds to any Bearer Set-up Request in step 2 or 4 with "*Transaction Pending*", no further action is taken until the BCF responds further.

If T44 expires at any time during the above procedures, the CSF initiates normal call termination procedures.

11) New clause 7.5.6 Polling at an international SN for IEPS calls

Add new clause 7.5.6 as follows:

7.5.6 Polling at an international SN for IEPS calls

For IEPS calls at an international SN, for the above cases 7.5.1 to 7.5.5 where the BCF has indicated a failure due to temporary resource unavailability to the Bearer Set-up Request, or there has been no reply to the Bearer Set-up Request, the following optional polling procedure is initiated in the CSF:

1) An ACM (no indication) with the inclusion of the generic notification parameter set to "*call completion delay*" is returned to the incoming side. If the IAM indicated "*COT to be expected*" then the sending of the ACM (no indication) is delayed until the COT has been received. A polling guard timer (T44) is started to prevent the CSF to be polling an IEPS call for an excessive time.
2) The CSF may immediately send a Bearer Set-up Request to a different BCF for the purpose of selecting a different BIWF. If the BCF indicates a failure due to temporary resource unavailability to the Bearer Set-up Request, or there has been no reply to the Bearer Set-up Request, this step may be repeated towards other BCFs.
3) If Bearer Set-up Failure due to temporary resource unavailability is indicated, or there is no reply to the Bearer Set-up Request, by all BCFs in step 2, the CSF shall start a polling timer (T45).
4) On expiry of T45, the CSF shall send a Bearer Set-up Request to the first BCF. If Bearer Set-up Failure due to temporary resource unavailability is indicated, or there is no reply to the Bearer Set-up request, steps 2 and 3 are repeated until a BCF indicates that resources are available. The time between successive polling attempts (T45) should be increased for each execution of step 3.

If the CSF receives a reply to the initial Bearer Set-up Request indicating "*Transaction Pending*", step 1 is executed and no further action is taken until the BCF responds further. If a BCF responds to any Bearer Set-up Request in step 2 or 4 with "*Transaction Pending*", no further action is taken until the BCF responds further.

If T44 expires at any time during the above procedures, the CSF initiates normal call termination procedures.

12) New clause 8.23 IEPS call information

Add new clause 8.23 as follows:

8.23 IEPS call information

8.23.1 Actions required at an outgoing international gateway SN or CMN

Where the CSF logic at the node determines that an IEPS call (as set out in 7.2.4.3 c and 7.2.5.3 b) requires IEPS information to be transported in the forward direction and based on bilateral agreement between administrations, the IEPS call information parameter shall be sent in the IAM. This parameter will contain the identity of the entity (the country or international network) originating the IEPS call, and the national priority level of the call. The priority level in the IEPS call information parameter will be the national priority level of the call in the entity originating the call. The priority level in the IEPS call information parameter is signalled in inverse order of the numerical value, i.e., the lower the numerical value is, the higher the priority. For example, numerical value 0 indicates the highest priority possible.

8.23.2 Actions required at an intermediate international SN or CMN

If an intermediate international SN or CMN receives a call with CPC set to IEPS, the call establishment proceeds with priority. The call is established with the CPC set as IEPS in the outgoing IAM. The IEPS call information parameter shall be passed on transparently. The SN or CMN shall not provide IEPS priority treatment if the CPC value is not IEPS, even if the optional IEPS call information parameter is present.

8.23.3 Actions required at an incoming international gateway SN or CMN

If an incoming international gateway SN or CMN receives a call with CPC set to IEPS, the call establishment proceeds with priority. On receipt of the IEPS call information parameter, the incoming international gateway SN or CMN may provide enhanced service features by analysing the contents of this parameter. The SN or CMN may provide a mapping of the IEPS priority level received from the entity (the country or international network) originating the IEPS call to that of the entity (the country or international network) of call destination. In case mapping is not implemented, the IEPS information parameter may be discarded, however, the call shall continue to be treated as a priority call. The call is established with the CPC set as IEPS or national specific information for IEPS call treatment in the outgoing IAM.

If the IEPS call information parameter is expected (due to bilateral agreements) but is not received for an IEPS call (i.e., CPC is set to IEPS), the call establishment proceeds with priority. If the IEPS call information parameter is received containing a value (country/international network code and/or priority level), which has not been bilaterally agreed for an IEPS call (i.e., CPC is set to IEPS), the call establishment proceeds with priority. The call is established with the CPC set as IEPS or national specific information for IEPS call treatment in the outgoing IAM. A default priority value will be used for the call in the entity of call destination. The SN or CMN shall not provide IEPS priority treatment if the CPC value is not IEPS, even if the optional IEPS call information parameter is present.

13) Annex A – Timers

Add the following timers to Table A.1:

Table A.1/Q.1902.4 – Timers in the BICC basic call protocol

Symbol	Time-out value	Cause for initiation	Normal termination	At expiry	Reference
T44	1-180 seconds	When the CSF receives failure due to temporary resource unavailability, or no reply, to the initial Bearer Set-up Request	Successful seizure of bearer	Initiate release procedures	7.4.6 7.5.6
T45	1-32 seconds, progressively increasing for each polling re-attempt (e.g., 2, 4, 6, 10, 16, 32)	When the CSF receives failure due to temporary resource unavailability, or no reply, to all Bearer Set-up Requests	–	Start polling by sending Bearer Set-up Request to first BCF	7.4.6 7.5.6

Signalling for IEPS support in CBC

ITU-T Rec. Q.1950 Amendment 1 (01/2006)

BEARER INDEPENDENT CALL BEARER CONTROL PROTOCOL: NEW ANNEX G – CALL BEARER CONTROL – INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

This amendment contains the procedures, formats and codes with regard to the Call Bearer Control function to support the International Emergency Preference Scheme (IEPS), which is specified in ITU-T Rec. E.106, in Bearer Independent Call Control (BICC) based networks.

G.1 Introduction

This annex describes the enhancements to the Q.1950 Call Bearer Control interface enabling the CSF to indicate to a BIWF that a particular context/call is being used for the International Emergency Preference Scheme.

G.2 References

G.2.1 Normative References

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

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

G.2.2 Informative References

–

G.3 Definitions

–

G.4 Abbreviations

IEPS International Emergency Preference Scheme

G.5 Definition of signalling flow objects

The following object is the signalling object to be carried by the commands in the transactions.

1) **IEPS indicator**: Indicates that the terminations and bearer connections in the specified context are associated with the features and techniques of ITU-T Rec. E.106 to be achieved.

G.6 Emergency service capability set

As per clause 6.

G.7 CBC procedures – Call-related

This clause contains the Call-Related procedures for IEPS when used in conjunction with Q.1950.

G.7.1 CSM transactions

The following transaction is used to indicate that a procedure is to be initiated by the CSM. The transaction leads to commands being sent across the CBC interface. See Table G.1.

Table G.1/Q.1950 – Call-related CSM originated transactions on the CBC interface

Transaction	Description
IEPS_Indication	This transaction is used to indicate to the BIWF that the IEPS service is used and IEPS handling should apply to the applicable context.

G.7.1.1 IEPS_Indication

When the transaction "IEPS_Indication" is required the following procedure is initiated.

An ADD.req, MOD.req or MOV.req command is sent with the following information.

1 ADD.req/MOD.req/MOV.req (..., IEPS_Indication) CSM to BIWF

Address Information	**Control information**	**Bearer information**
As per flow (1) 7.1.1/Q.1950 Prepare_BNC_Notify or As per flow (1) 7.1.2/Q.1950 Establish_BNC_Notify	As per flow (1) 7.1.1/Q.1950 Prepare_BNC_Notify With the following additions: If Context Requested & IEPS Call: IEPS Indicator OR: As per flow (1) 7.1.2/Q.1950 Establish_BNC_Notify With the following additions: If Context is NOT provided & IEPS Call: IEPS Indicator	As per flow (1) 7.1.1/Q.1950 Prepare_BNC_Notify or As per flow (1) 7.1.2/Q.1950 Establish_BNC_Notify

Upon reception of the command, the BIWF shall:

- If the IEPS Indicator is present, apply preferential handling according to E.106, with respect to all resources associated with the specified context. Mapping to any priority values present in the relevant bearer control protocol, including the application of pre-emption, is out of scope of this Recommendation.
- Apply the procedures of 7.1.1/Q.1950 Prepare_BNC_Notify or 7.1.2/Q.1950 Establish_BNC_Notify as applicable.

Upon completion of processing command (1) an ADD.resp, MOD.resp or MOV.resp command (2) is sent.

2 ADD.resp/MOD.resp/MOV.resp BIWF to CSM

Address Information	Control information	Bearer information
As per flow (1) 7.1.1/Q.1950 Prepare_BNC_Notify or As per flow (1) 7.1.2/Q.1950 Establish_BNC_Notify	As per flow (1) 7.1.1/Q.1950 Prepare_BNC_Notify or As per flow (1) 7.1.2/Q.1950 Establish_BNC_Notify	As per flow (1) 7.1.1/Q.1950 Prepare_BNC_Notify or As per flow (1) 7.1.2/Q.1950 Establish_BNC_Notify

G.7.2 BIWF transactions

–

G.8 Formats and codes

This clause outlines the encoding of the IEPS when used with the CBC protocol.

G.8.1 Formats and codes – General

As per 10.1.

G.8.2 Formats and codes – Commands

As per 10.2.

G.8.3 Formats and codes – Signalling objects

See Table G.2.

Table G.2/Q.1950 – CBC signalling object to H.248.1 coding mapping table

CBC signalling object	H.248.1 descriptor	H.248.1 coding
IEPS Indicator	NA	6.1.1/H.248.1 IEPS Indicator encoded as per Annexes A/H.248.1 (IEPS Call Ind) or B/H.248.1 (IEPS Value) context attribute.

Signalling for IEPS support in ATM AAL2

ITU-T Rec. Q.2630.3 Amendment 1 (01/2006)

AAL TYPE 2 SIGNALLING PROTOCOL – CAPABILITY SET 3: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.2630.3 (2003) in order to accommodate these needs. This amendment is designed to be compatible with implementations conforming to ITU-T Rec. Q.2630.3 (2003).

1) Clause 2.1

Revise clause 2.1 as follows:

2.1 Normative references

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

[1] ITU-T Recommendation I.363.2 (2000), *B-ISDN ATM Adaptation Layer specification: Type 2 AAL*.

[2] ITU-T Recommendation I.361 (1999), *B-ISDN ATM layer specification*.

[3] ITU-T Recommendation X.200 (1994), *Information technology – Open Systems Interconnection – Basic reference model: The basic model*.

[4] ITU-T Recommendation X.210 (1993), *Information technology – Open Systems Interconnection – Basic reference model: Conventions for the definition of OSI services*.

[5] ITU-T Recommendation X.213 (2001), *Information technology – Open Systems Interconnection – Network service definitions*.

[6] ITU-T Recommendation Q.850 (1998), *Usage of cause and location in DSS 1 and SS No. 7 ISUP*.

[7] ITU-T Recommendation Q.2610 (1999), *Usage of cause and location in B-ISDN User Part and DSS 2*.

[8] ITU-T Recommendation I.366.2 (1999), *AAL type 2 service specific convergence sublayer for trunking*.

[9] ITU-T Recommendation I.366.1 (1998), *Segmentation and Reassembly Service Specific Convergence Sublayer for the AAL type 2*.

[10] ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan*.

[11] IEEE Standard 802-2001, *IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture*.

[12] ITU-T Recommendation Q.2150.0 (2001), *Generic signalling transport service*.

[13] ITU-T Recommendation I.356 (2000), *B-ISDN ATM layer cell transfer performance*.

[14] ITU-T Recommendation I.366.2 (2000), *AAL type 2 service specific convergence sublayer for narrowband services*.

[15] ITU-T Recommendation Q.2630.1 (1999), *AAL type 2 signalling protocol – Capability Set 1*.

[16] ITU-T Recommendation Q.2630.2 (2000), *AAL type 2 signalling protocol – Capability Set 2*.

[17] ITU-T Recommendation E.412 (2003), *Network management controls*.

[18] ITU-T Recommendation Q.542 (1993), *Digital exchange design objectives – Operations and maintenance*.

[19] ITU-T Recommendation I.378 (2002), *Traffic control and congestion control at the ATM Adaptation Layer Type 2*.

2) Clause 4

Add the following new abbreviations alphabetically:

4 Abbreviations

A2P	AAL type 2 Path Identifier
A2SU	AAL type 2 Served User
AAL	ATM Adaptation Layer
ACC	Automatic Congestion Control
AESA	ATM End System Address
AMR	Adaptive Multi-rate Codec
ANI	Adjacent AAL type 2 Node Identifier
ATM	Asynchronous Transfer Mode
ATM VCC	ATM Virtual Channel Connection
BCD	Binary Coded Decimal
BLC	Block Confirm Message
BLO	Block Request Message
CAS	Channel Associated Signalling
CAU	Cause Parameter
CEID	AAL type 2 Connection Element Identifier
CFN	Confusion Message
CID	Channel Identifier

CMD	Circuit Mode Data
CP	Connection Priority
CPHL	CPS Packet Header Overhead Length
CPS	(AAL type 2) Common Part Sublayer
CS	Capability Set
CS-1	Capability Set 1 (ITU-T Rec. Q.2630.1 [15])
CS-2	Capability Set 2 (ITU-T Rec. Q.2630.2 [16])
CS-3	Capability Set 3 (this Recommendation)
DA2EA	Destination AAL type 2 Service Endpoint Address (Note 1)
DESEA	Destination E.164 Service Endpoint Address Parameter (Note 1)
DNSEA	Destination NSAP Service Endpoint Address Parameter (Note 1)
DSAID	Destination Signalling Association Identifier
DTMF	Dual Tone Multi-Frequency
ECF	Establish Confirm Message
ERQ	Establish Request Message
FAX	Demodulated Facsimile Data
FBW	Fixed Bandwidth Transfer Capability
FRM	Frame Mode Data
GST	Generic Signalling Transport
HBx	Header Bit Rate associated with x
HC	Hop Counter
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
LB	Loopback
LC	Link Characteristics (Note 2)
LM	Layer Management
LSB	Least Significant Bit
M	Mandatory
MF-R1	Multi-Frequency R1
MF-R2	Multi-Frequency R2
MOA	Modification Acknowledge message
MOD	Modification Request message
MOR	Modification Reject message

MSB	Most Significant Bit
MSLC	Modify Support for Link Characteristics
MSSSI	Modify Support for SSCS Information
MTP3b	Message Transfer Part level 3 using ITU-T Rec. Q.2140 [29]
NF	Nodal Function
NNI	Network-Network Interface
NSAP	Network Service Access Point
O	Optional
OA2EA	Origination AAL type 2 Service Endpoint Address
OESEA	Origination E.164 Service Endpoint Address Parameter
ONSEA	Origination NSAP Service Endpoint Address Parameter
OSAID	Originating Signalling Association Identifier (Parameter)
OUI	Organizational Unique Identifier
PFBW	Preferred FBW
PLC	Preferred Link Characteristics
PSSCS	Preferred SSCS Information
PSSIAE	Preferred Service Specific Information (Audio Extended)
PSSIME	Preferred Service Specific Information (Multirate Extended)
PT	Path Type
PTC	Preferred Transfer Capability
PVBWS	Preferred VBWS
PVBWT	Preferred VBWT
PVC	Permanent Virtual Channel
RC	Rate Control
REL	Release Request Message
RES	Reset Request Message
RLC	Release Confirm Message
RSC	Reset Confirm Message
SAAL	ATM Adaptation Layer for Signalling
SAID	Signalling Association Identifier
SAP	Service Access Point
SAR	Segmentation and Reassembly (Sublayer)
SDL	Specification and Description Language
SDU	Service Data Unit
SPVC	Soft PVC

SSCOP	Service Specific Connection Oriented Protocol
SSCS	Service Specific Convergence Sublayer
SSCS	SSCS Information
SSIA	Service Specific Information (Audio) Parameter
SSIAE	Service Specific Information (Audio Extended)
SSIM	Service Specific Information (Multirate) Parameter
SSIME	Service Specific Information (Multirate Extended)
SSISA	Service Specific Information (SAR-assured) Parameter
SSISU	Service Specific Information (SAR-unassured) Parameter
SSSAR	Segmentation and Reassembly Service Specific Convergence Sublayer
STC	Signalling Transport Converter
SUCI	Served User Correlation ID
SUGR	Served User Generated Reference
SUT	Served User Transport
SVC	Switched Virtual Channel
SYN	Synchronization of change in SSCS operation
TAR	Temporary Alternative Routing
TC	Transfer Capability
TCC	TAR Controlled Connection
TCI	Test Connection Indication
TCS	Transfer Capability Support
TED	Transmission Error Detection
UBC	Unblock Confirm Message
UBL	Unblock Request Message
UNI	User-Network Interface
UU	User-user
VBWS	Variable Bandwidth Stringent Transfer Capability
VBWT	Variable Bandwidth Tolerant Transfer Capability
VCC	Virtual Channel Connection
VPC	Virtual Path Connection

NOTE 1 – In ITU-T Recs Q.2630.1 [15] and Q.2630.2 [16], the abbreviation A2EA was used instead of DA2EA, ESEA instead of DESEA, and NSEA instead of DNSEA.

NOTE 2 – In ITU-T Rec. Q.2630.1 [15], the abbreviation ALC was used instead of LC.

3) Clause 5.1.2

Revise clause 5.1.2 as follows:

5.1.2 Primitives between AAL type 2 signalling entities and the AAL type 2 served user

The A2SU-SAP primitives are used:

1) by the originating served user to initiate AAL type 2 connection establishment and by the originating and destination served users to initiate the release of a connection;
2) by the AAL type 2 signalling entities to indicate an incoming connection to the destination served user and notifying either the originating or destination served user of the release of a connection;
3) by the modification sending served user to originate, and the modification receiving served user to respond to, an AAL type 2 connection resource modification request; and
4) by the AAL type 2 signalling entities to indicate a modification of the AAL type 2 connection resource to the modification receiving served user and notify the modification originating served user of the successful or unsuccessful modification.

NOTE – When sending a primitive between the signalling protocol and its user, the primitive needs to be associated with a particular AAL type 2 connection instance. The mechanism used for this binding is considered to be an implementation detail and therefore is outside the scope of this Recommendation.

The services are provided through the transfer of primitives which are summarized in Table 5-1, and are defined after the table.

The AAL type 2 served user passes information in parameters in the primitives. Some of those parameters are mandatory and some are optional; the appropriate usage of the parameters is described in clause 8.

Table 5-1/Q.2630.3 – Primitives and parameters exchanged between the AAL type 2 signalling entities and the AAL type 2 served user

Primitive Generic Name	Type			
	Request	Indication	Response	Confirm
ESTABLISH	DA2EA, OA2EA, SUGR, SUT, TC, PTC, TCS, LC, PLC, MSLC, SSCS, PSSCS, MSSSI, PT, II, CP, TCI	OA2EA, SUGR, SUT, TC, PTC, TCS, LC, PLC, MSLC, SSCS, PSSCS, MSSSI, PT, II, CP, TCI	Not defined	TCS, MSLC, MSSSI
RELEASE	Cause	Cause	Not defined	Cause
MODIFY	TC, LC, SSCS, SUCI	TC, LC, SSCS, SUCI	SUCI	SUCI
MODIFY-REJECT	Not defined	Not defined	Not defined	Cause

a) **ESTABLISH.request**

This primitive is used by the AAL type 2 served user to initiate the establishment of a new AAL type 2 connection, and optionally request the capability for subsequent modification to be performed on the requested connection.

b) **ESTABLISH.indication**

This primitive is used by the AAL type 2 signalling entities to indicate that an incoming connection has been successfully established, and optionally indicate that the incoming connection is capable of subsequent modification.

c) **ESTABLISH.confirm**

This primitive is used by the AAL type 2 signalling entities to indicate that the connection (which was previously requested by the served user) has successfully been established and optionally indicate that the established connection is capable of subsequent modification.

d) **RELEASE.request**

This primitive is used by the AAL type 2 served user to initiate clearing of an AAL type 2 connection.

e) **RELEASE.indication**

This primitive is used by the AAL type 2 signalling entities to indicate that an AAL type 2 connection has been released.

f) **RELEASE.confirm**

This primitive is used as a negative acknowledgement for an ESTABLISH.request.

g) **MODIFY.request**

This primitive is used by the AAL type 2 served user to originate the modification of the AAL type 2 connection resource.

h) **MODIFY.indication**

This primitive is used by the AAL type 2 signalling entities to indicate that the modification of the AAL type 2 connection resource has been successfully performed.

i) **MODIFY.response**

This primitive is used by the AAL type 2 served user to respond to the modification of the AAL type 2 connection resource.

j) **MODIFY.confirm**

This primitive is used by the AAL type 2 signalling entities to indicate that the AAL type 2 connection resource modification (which was previously requested by the served user) has successfully been performed.

k) **MODIFY-REJECT.confirm**

This primitive is used by the AAL type 2 signalling entities to indicate that the AAL type 2 connection resource modification (which was previously requested by the served user) has been rejected.

4) Clause 5.1.3

Revise clause 5.1.3 as follows:

5.1.3 Parameters between AAL type 2 signalling entities and the AAL type 2 served user

a) **Destination AAL type 2 Service Endpoint Address (DA2EA)**

This parameter carries the service endpoint address of the destination. It can have the form of an E.164 address or an NSAP address.

b) **Origination AAL type 2 Service Endpoint Address (OA2EA)**

This parameter carries the service endpoint address of the origination. It can have the form of an E.164 address or an NSAP address.

c) **Served User Generated Reference (SUGR)**

This parameter carries a reference provided by the originating AAL type 2 served user and this reference is transported unmodified to the destination served user.

d) **Served User Transport (SUT)**

This parameter carries the served user data that is transported unmodified to the destination served user.

e) **Transfer Capability (TC)**

This parameter gives an indication of the AAL type 2 transfer capability required for the AAL type 2 connection. This parameter can have the form of either:

- Fixed Bandwidth Transfer Capability; or
- Variable Bandwidth Stringent Transfer Capability; or
- Variable Bandwidth Tolerant Transfer Capability.

f) **Preferred Transfer Capability (PTC)**

This parameter gives an indication that the AAL type 2 Transfer Capability shall be set as indicated in this parameter if the modification of the AAL type 2 Transfer Capability is permitted. This parameter can have the form of either:

- Preferred Fixed Bandwidth Transfer Capability; or
- Preferred Variable Bandwidth Stringent Transfer Capability; or
- Preferred Variable Bandwidth Tolerant Transfer Capability.

g) **Transfer Capability Support (TCS)**

This parameter gives an indication whether Transfer Capabilities are supported by all AAL type 2 nodes of the AAL type 2 connection.

h) **Link Characteristics (LC)**

This parameter gives an indication of the resources required for the AAL type 2 connection and is used only for AAL type 2 path selection and connection admission control.

i) **Preferred Link Characteristics (PLC)**

This parameter gives an indication that the Link Characteristics shall be set as indicated in this parameter if the modification of the Link Characteristics is permitted.

j) **Modify Support for Link Characteristics (MSLC)**

This parameter gives an indication that the AAL type 2 Link Characteristics of the AAL type 2 connection may need to be modified during the lifetime of the AAL type 2 connection (ESTABLISH.request) or is permitted to be modified (ESTABLISH.indication and ESTABLISH.confirm).

k) **SSCS Information (SSCS)**

This parameter identifies the type and the capabilities of an AAL type 2 SSCS protocol. This parameter can have the form of either:

- Service Specific Information (Multirate) (see ITU-T Rec. I.366.2 [14]);
- Service Specific Information (Audio) (see ITU-T Rec. I.366.2 [14]);
- Service Specific Information (Multirate Extended) (see Note);
- Service Specific Information (Audio Extended) (see Note); or
- Service Specific Information (SAR) (see ITU-T Rec. I.366.1 [9]) with or without the additional parameters necessary for the assured data transfer.

NOTE – Multirate Extended and Audio Extended are used in this Recommendation to support the services of the U-Plane definitions of the 2000 version of ITU-T Rec. I.366.2 [14]. The (non-extended) Multirate and Audio are retained for backward compatibility with ITU-T Rec. Q.2630.1 [15]. For example, the Audio Extended form of the SSCS Information parameter in this Recommendation (see 7.4.19) adds support for LB, RC, and SYN that were added as U-Plane functions in the 2000 version of ITU-T Rec. I.366.2 [14].

l) **Preferred SSCS Information (PSSCS)**

This parameter gives an indication that the SSCS Information shall be set as indicated in this parameter if the modification of the SSCS Information is permitted. This parameter can have the form of either:

- Preferred Service Specific Information (Multirate Extended) (see Note); or
- Preferred Service Specific Information (Audio Extended) (see Note).

Modification of Frame Mode Data as specified in ITU-T Rec. I.366.2 [14], or modification of SAR as specified in ITU-T Rec. I.366.1 [9] is outside the scope of this Recommendation.

m) **Modify Support for SSCS Information (MSSSI)**

This parameter gives an indication that the SSCS Information of the AAL type 2 connection may need to be modified during the lifetime of the AAL type 2 connection (ESTABLISH.request) or are permitted to be modified (ESTABLISH.indication and ESTABLISH.confirm).

n) **Path Type (PT)**

This parameter indicates a request for an AAL type 2 path with a specified Quality of Service.

o) **Connection Priority (CP)**

This parameter carries information sent in the forward direction to indicate the priority level of the connection request.

p) **Test Connection Indicator (TCI)**

By its presence, this parameter indicates that the AAL type 2 connection to be established is a test connection.

q) **Cause**

This parameter describes the reason for the release of the AAL type 2 connection. It also may indicate the reason why an AAL type 2 connection could not be established or a modification was rejected.

r) **Served User Correlation ID (SUCI)**

This parameter carries the SSCS correlation ID (as specified in ITU-T Rec. I.366.2 [14]) during the modification of SSCS information and is transported unmodified to the destination or origination served user.

5) Clause 7.2.2

Revise clause 7.2.2 as follows:

7.2.2 Parameters of the AAL type 2 signalling protocol messages

The parameters of the AAL type 2 signalling protocol messages are shown in Table 7-6. The indications of "mandatory" and "optional" are for information only. The authoritative definition is given in clause 8 and Annex C. If any difference between the indications in this clause and the definitions in clause 8 and Annex C exists, the definitions in clause 8 take precedence.

Multiple presence of the same parameter in a single message is not permitted.

Table 7-6/Q.2630.3 – (part 1 of 2)
Parameters of the AAL type 2 signalling protocol messages

Parameter	Message						
	ERQ	ECF	REL	RLC	MOD	MOA	MOR
Automatic Congestion Control	–	–	O	O	–	–	–
Cause	–	–	M	Note 12	–	–	M
Connection Element Identifier	M	–	–	O	–	–	–
Connection Priority	O	–	–	–	–	–	–
Destination E.164 Service Endpoint Address	Note 2	–	–	–	–	–	–
Destination NSAP Service Endpoint Address	Note 2	–	–	–	–	–	–
Destination Signalling Association Identifier (Note 1)	Note 3	M	M	M	M	M	M
Hop Counter	O	–	–	–	–	–	–
Link Characteristics	Note 4	–	–	–	Note 4	–	–
Modify Support for Service Specific Information	Notes 4, 16	Note 4	–	–	–	–	–
Modify Support for Link Characteristics	Notes 4, 14	Note 4	–	–	–	–	–
Originating Signalling Association Identifier	M	M	–	–	–	–	–
Origination E.164 Service Endpoint Address	Note 5	–	–	–	–	–	–
Origination NSAP Service Endpoint Address	Note 5	–	–	–	–	–	–
Path Type	Note 6	–	–	–	–	–	–
Preferred Link Characteristics	Notes 4, 15	–	–	–	–	–	–
Preferred Service Specific Information (Audio Extended)	Notes 4, 7	–	–	–	–	–	–
Preferred Service Specific Information (Multirate Extended)	Notes 4, 7	–	–	–	–	–	–
Preferred Transfer Capability (FBW)	Notes 4, 8	–	–	–	–	–	–
Preferred Transfer Capability (VBWS)	Notes 4, 8	–	–	–	–	–	–
Preferred Transfer Capability (VBWT)	Notes 4, 8	–	–	–	–	–	–
Served User Correlation ID	–	–	–	–	O	O	–
Served User Generated Reference	O	–	–	–	–	–	–
Served User Transport	O	–	–	–	–	–	–
Service Specific Information (Audio Extended)	Notes 9, 10	–	–	–	Notes 13, 17	–	–
Service Specific Information (Audio)	Notes 4, 9, 10	–	–	–	–	–	–
Service Specific Information (Multirate Extended)	Notes 9, 10	–	–	–	Notes 13, 17	–	–

Table 7-6/Q.2630.3 – (part 1 of 2)
Parameters of the AAL type 2 signalling protocol messages *(end)*

Parameter	Message						
	ERQ	ECF	REL	RLC	MOD	MOA	MOR
Service Specific Information (Multirate)	Notes 4, 9, 10	–	–	–	–	–	–
Service Specific Information (SAR-assured)	Note 9	–	–	–	–	–	–
Service Specific Information (SAR-unassured)	Note 9	–	–	–	–	–	–
TAR Controlled Connection	O	–	–	–	–	–	–
Test Connection Indicator	O	–	–	–	–	–	–

Table 7-6/Q.2630.3 – (part 1 of 2)
Parameters of the AAL type 2 signalling protocol messages

Parameter	Message						
	ERQ	ECF	REL	RLC	MOD	MOA	MOR
Transfer Capability (FBW)	Note 11	–	–	–	Notes 13, 17	–	–
Transfer Capability (VBWS)	Note 11	–	–	–	Notes 13, 17	–	–
Transfer Capability (VBWT)	Note 11	–	–	–	Notes 13, 17	–	–
Transfer Capability Support (TCS)	Note 4	Note 4	–	–	–	–	–

M Mandatory parameter
O Optional parameter
– Parameter not present

NOTE 1 – This row designates the Destination Signalling Association Identifier field in the message header.

NOTE 2 – Exactly one of these parameters must be present in an instance of the message.

NOTE 3 – The Destination Signalling Association Identifier field contains the value "unknown".

NOTE 4 – This parameter is only used for backward compatibility, i.e., for interworking with AAL type 2 nodes that conform only to ITU-T Recs Q.2630.1 [15] or Q.2630.2 [16] (see Annex C).

NOTE 5 – At most one of these parameters is present in an instance of the message.

NOTE 6 – If the path type parameter is not included, the path type shall be considered to be the network default stringent QoS class.

NOTE 7 – This parameter may only be included if "Modify Support for Service Specific Information" is included; at most one of these parameters is present in an instance of the message. If present it must refer to the same service specific information as the Service Specific Information parameter present in the same Establish Request message, i.e., Audio or Multirate.

NOTE 8 – This parameter must be included if a "Preferred Link Characteristics" and/or a "Preferred Service Specific Information" is included. At most one of these parameters is present in an instance of the message. If present it must refer to the same transfer capability as the Transfer Capability parameter present in the same Establish Request message.

NOTE 9 – At most one of these parameters is present in an instance of the message.

NOTE 10 – If the Modify Support for Service Specific Information parameter is included, this parameter shall also be included.

NOTE 11 – Exactly one of these parameters is present in an instance of the message.

NOTE 12 – The "Cause" parameter is present in the Release Confirm message if:
a) the RLC is used to reject a connection establishment; or
b) the cause reports unrecognized information received in the REL message.

Table 7-6/Q.2630.3 – (part 1 of 2)
Parameters of the AAL type 2 signalling protocol messages *(end Notes)*

NOTE 13 – At most one of these parameters is present in an instance of the message, and only the same parameter that was present in the Establish Request message may be present.
NOTE 14 – This parameter may be present only if the parameter "Link Characteristics" is present also.
NOTE 15 – This parameter may be present only if the parameter "Modify Support for Link Characteristics" is present also.
NOTE 16 – This parameter may be present only if one of the parameters "Service Specific Information (Audio)", "Service Specific Information (Audio Extended)", "Service Specific Information (Multirate)", and "Service Specific Information (Multirate Extended)" is present also.
NOTE 17 – At least one of these parameters is present in an instance of the message.

Table 7-6/Q.2630.3 – (part 2 of 2)
Parameters of the AAL type 2 signalling protocol messages

Parameter	Message						
	RES	RSC	BLO	BLC	UBL	UBC	CFN
Cause	–	Note 4	–	Note 4	–	Note 4	M
Connection Element Identifier	M	–	M Note 3	–	M Note 3	–	–
Destination Signalling Association Identifier (Note 1)	Note 2	M	Note 2	M	Note 2	M	M
Originating Signalling Association Identifier	M	–	M	–	M	–	–

M Mandatory parameter
O Optional parameter
– Parameter not present

NOTE 1 – This row designates the Destination Signalling Association Identifier field in the message header.

NOTE 2 – The Destination Signalling Association Identifier field contains the value "unknown".

NOTE 3 – The Channel Identifier field is set to "Null", but the Path Identifier includes a value identifying an AAL type 2 path.

NOTE 4 – The "Cause" parameter is present only if the cause reports unrecognized information received.

The identifiers of the AAL type 2 message parameters are defined in Table 7-7.

Table 7-7/Q.2630.3 – Identifiers of the AAL type 2 message parameters

AAL type 2 Parameter	Ref.	Acronym	Identifier
Automatic Congestion Control	7.3.25	ACC	0 0 0 1 1 0 0 0
Cause	7.3.1	CAU	0 0 0 0 0 0 0 1
Connection Element Identifier	7.3.2	CEID	0 0 0 0 0 0 1 0
Connection Priority	7.3.26	CP	0 0 0 1 1 0 0 1
Destination E.164 Service Endpoint Address	7.3.3	DESEA	0 0 0 0 0 0 1 1
Destination NSAP Service Endpoint Address	7.3.4	DNSEA	0 0 0 0 0 1 0 0
Hop Counter	7.3.27	HC	0 0 0 1 1 0 1 0
Link Characteristics (Note)	7.3.5	LC	0 0 0 0 0 1 0 1
Modify Support for Link Characteristics (Note)	7.3.20	MSLC	0 0 0 0 1 1 1 0

Table 7-7/Q.2630.3 – Identifiers of the AAL type 2 message parameters *(end)*

AAL type 2 Parameter	Ref.	Acronym	Identifier
Modify Support for Service Specific Information (Note)	7.3.21	MSSSI	0 0 0 0 1 1 1 1
Originating Signalling Association Identifier	7.3.6	OSAID	0 0 0 0 0 1 1 0
Origination E.164 Service Endpoint Address	7.3.23	OESEA	0 0 0 1 1 0 1 1
Origination NSAP Service Endpoint Address	7.3.24	ONSEA	0 0 0 1 0 1 0 1
Path Type	7.3.14	PT	0 0 0 1 0 0 0 0
Preferred Link Characteristics (Note)	7.3.19	PLC	0 0 0 1 0 0 0 1
Preferred Service Specific Information (Audio Extended) (Note)	7.3.17	PSSIAE	0 0 0 1 0 0 1 0
Preferred Service Specific Information (Multirate Extended) (Note)	7.3.18	PSSIME	0 0 0 1 0 0 1 1
Preferred Transfer Capability (FBW) (Note)	7.3.29	PFBW	0 0 0 1 1 1 0 0
Preferred Transfer Capability (VBWS) (Note)	7.3.30	PVBWS	0 0 0 1 1 1 0 1
Preferred Transfer Capability (VBWT) (Note)	7.3.31	PVBWT	0 0 0 1 1 1 1 0
Served User Correlation ID	7.3.22	SUCI	0 0 0 1 0 1 0 0
Served User Generated Reference	7.3.7	SUGR	0 0 0 0 0 1 1 1
Served User Transport	7.3.8	SUT	0 0 0 0 1 0 0 0
Service Specific Information (Audio Extended)	7.3.15	SSIAE	0 0 0 1 0 1 1 0
Service Specific Information (Audio) (Note)	7.3.9	SSIA	0 0 0 0 1 0 0 1
Service Specific Information (Multirate Extended)	7.3.16	SSIME	0 0 0 1 0 1 1 1
Service Specific Information (Multirate) (Note)	7.3.10	SSIM	0 0 0 0 1 0 1 0
Service Specific Information (SAR-assured)	7.3.11	SSISA	0 0 0 0 1 0 1 1
Service Specific Information (SAR-unassured)	7.3.12	SSISU	0 0 0 0 1 1 0 0
TAR Controlled Connection	7.3.28	TCC	0 0 0 1 1 1 1 1
Test Connection Indicator	7.3.13	TCI	0 0 0 0 1 1 0 1
Transfer Capability (FBW)	7.3.32	FBW	0 0 1 0 0 0 0 0
Transfer Capability (VBWS)	7.3.33	VBWS	0 0 1 0 0 0 0 1
Transfer Capability (VBWT)	7.3.34	VBWT	0 0 1 0 0 0 1 0
Transfer Capability Support (Note)	7.3.35	TCS	0 0 1 0 0 0 1 1
NOTE – In this Recommendation, this parameter is only used for backward compatibility, i.e., for interworking with AAL type 2 nodes that conform only to ITU-T Recs Q.2630.1 [15] or Q.2630.2 [16].			

6) New clause 7.3.36

Add the following new clause:

7) Clause 8

Revise clause 8 as follows:

8 Procedure of the AAL type 2 signalling protocol

Before an ATM VCC (AAL type 2 path) is put into service between a pair of adjacent AAL type 2 nodes, certain actions need to be performed. An identifier called the AAL type 2 path identifier is assigned to the ATM VCC. This identifier is used to refer to the ATM VCC in the AAL type 2 signalling protocol messages. The AAL type 2 path identifier shall uniquely identify the ATM VCC between the two adjacent AAL type 2 nodes.

On any ATM VCC used for AAL type 2 connections, all CID values from "8" to "255" are available for assignment.

Any time a new ATM VCC is put into service, the ownership of the ATM VCC shall be determined before AAL type 2 connections are established in it. In case of switched ATM VCC, the owner of the VCC shall be the AAL type 2 node that initiated the establishment of the VCC. In case of PVC and soft PVC, it is the responsibility of the management system to determine the owner of the VCC.

The nodal function is informed by layer management of a newly established AAL type 2 path by the use of the ADD-PATH.indication primitive containing the adjacent AAL type 2 node identifier, the AAL type 2 path identifier, and the ownership. The nodal function is informed by layer management of the removal of an AAL type 2 path by use of the REMOVE-PATH.indication primitive containing the adjacent AAL type 2 node identifier and the AAL type 2 path identifier.

In order to minimize the likelihood of CID collision, the following CID allocation mechanism shall be used:

- if the AAL type 2 node owns the AAL type 2 path that carries the new connection, it allocates CID values from CID value 8 upwards; and
- if the AAL type 2 node does not own the AAL type 2 path that carries the new connection, it allocates CID values from CID value 255 downwards.

Each AAL type 2 connection request (regardless of coming directly from an AAL type 2 served user or from an adjacent AAL type 2 node) shall contain an AAL type 2 service endpoint address which indicates the destination of the intended AAL type 2 connection instance. This information is used to route the AAL type 2 connection via the AAL type 2 network to its destination service endpoint. In capability set 3, the supported address formats are: NSAP and E.164.

It is up to the application area or the operator of a particular network to decide what addressing plan is used in the AAL type 2 network. The addressing plan in the AAL type 2 network can be a reuse of the addressing plan in the underlying ATM network but it can also be an independent addressing plan defined exclusively for the AAL type 2 network.

NOTE – Causes in the procedures defined in clause 8 specify which ITU-T standardized code should be used in cause parameters of AAL type 2 signalling protocol messages. Implementation dependent non-standardized causes may be used for AAL type 2 signalling entity internal processing and for A2SU-SAP and LM-SAP cause primitive parameters.

The following procedures may be supported as a network option:

a) Connection priority;

b) Automatic congestion control (see ITU-T Rec. Q.542 [18]);

c) Hop Counter Procedure;

d) Temporary Alternative Routing Procedure (see ITU-T Rec. E.412 [17]).

8) Clause 8.2.1.1.1.1

Revise clause 8.2.1.1.1.1 as follows:

8.2.1.1.1.1 Actions at the originating AAL type 2 service endpoint

When the nodal function receives an ESTABLISH.request primitive from the AAL type 2 served user, the following parameters are mandatory:

- Destination Endpoint Address; and
- Transfer Capability.

When the nodal function receives an ESTABLISH.request primitive from the AAL type 2 served user, the restrictions on the optionality of the parameters used only for interworking with CS-1 or CS-2 nodes is described in Annex C. These optional parameters are the following:

- The Preferred Transfer Capability;
- Transfer Capability Support;
- Link Characteristics;
- Preferred Link Characteristics;
- Modify Support for Link Characteristics;
- Preferred Service Specific Information;
- Modify Support for Service Specific Information;
- Service Specific Information (Audio); and
- Service Specific Information (Multirate).

No optionality restrictions apply to the other parameters.

The nodal function analyses the routing information and selects a route with sufficient AAL type 2 path resources on a path with the requested path type (or network default if the path type is not specified) to the succeeding AAL type 2 node. It then selects an AAL type 2 path from within that route which is able to accommodate the new connection.

NOTE 1 – Routing typically is based on:

- Addressing information;
- The Test Connection Indicator;
- Transfer Capability;
- Requested Path Type;
- Automatic congestion control and the congestion level in the routing tables; and
- Temporary Alternative Routing control (see ITU-T Rec. E.412 [17]).

When the nodal functions selects a route, the connection priority information, if received from the AAL Type 2 served user is used to select a route that has sufficient AAL type 2 path resources to the succeeding AAL type 2 node.

Under the normal condition, when the network is not congested and the AAL Type 2 service endpoint has the necessary resources to complete it, the connection establishment is processed without special treatments.

NOTE 2 – In times of network congestion, when the AAL Type 2 service endpoint does not have sufficient resources to complete all of the incoming connection establishment requests, as one option, the AAL Type 2 service endpoint may give preferential treatments based on the priority level.

NOTE 3 – The preferential treatment should include access to reserved network resources, e.g.:

- the highest priority connections, are given access to available network resources including the resources reserved for highest priority connections;
- the second highest priority connections are given access to available network resources including the resources reserved for the second highest priority connections, except for the resources reserved for the highest priority connections, and so on.

NOTE 4 – Allocation of reserved network resources to specific priority levels is implementation specific, and is not a subject for standardization.

AAL type 2 service endpoint internal resources are allocated for the new connection from the originating AAL type 2 served user to the outgoing AAL type 2 path. The connection priority information, if received, is taken into consideration when allocating these resources.

On the selected outgoing AAL type 2 path, the CID and other resources (e.g., indicated by the Transfer Capability parameter) are allocated for the outgoing AAL type 2 link. The handling of interworking with CS-1 and CS-2 nodes is specified in Annex C.

The following parameters – if they were conveyed by the originating AAL type 2 served user – shall not be modified by the nodal function:

- the Destination Service Endpoint Address;
- the Origination Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the Transfer Capability;
- the Preferred Transfer Capability;
- the Transfer Capability Support;
- the Link Characteristics;
- the Preferred Link Characteristics;
- the Modify Support for Link Characteristics;
- the SSCS Information;
- the Preferred SSCS Information;
- the Modify Support for SSCS Information;
- the Path Type;
- the Connection Priority; and
- the Test Connection Indicator.

The following parameters – if they were conveyed by the originating AAL type 2 served user – have significance to the served user only; therefore, they shall not be examined by the nodal function:

- the Origination Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the SSCS Information;
- the Preferred SSCS Information; and
- the Modify Support for SSCS Information.

An outgoing protocol entity instance is invoked and the following parameters are passed to it:

- the Destination AAL type 2 Service Endpoint Address;
- the Transfer Capability;
- the AAL type 2 Path Identifier; and
- a CID value.

The nodal function shall pass the following parameters to the outgoing protocol entity instance only if they were conveyed by the originating AAL type 2 served user:

- the Origination AAL type 2 Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the Preferred Transfer Capability;
- the Transfer Capability Support;
- the Link Characteristics;
- the Preferred Link Characteristics;
- the Modify Support for Link Characteristics;
- the SSCS Information;
- the Preferred SSCS Information;
- the Modify Support for SSCS Information;
- the Path Type;

••

- the Connection Priority; and
- the Test Connection Indicator.

If the Temporary Alternative Routing control is applied a "TAR controlled connection" indication shall be passed to the outgoing protocol entity instance.

If the hop counter procedure has been activated a Hop Counter containing an initial count value shall be passed to the outgoing protocol entity instance. The initial count value of the Hop Counter shall be provisioned by the network operator on a per AAL type 2 node basis (31 maximum).

NOTE 5 – Through-connection at AAL type 2 service endpoints is not specified by this Recommendation. It may be controlled by the AAL type 2 served user.

After receiving an indication of the successful AAL type 2 connection setup from the outgoing protocol entity instance, an ESTABLISH.confirm primitive is sent to the AAL type 2 served user. If a Transfer Capability Support parameter, a Modify Support for Link Characteristics, or a Modify Support for SSCS Information parameter was received from the outgoing protocol instance, the respective parameter shall be included in the ESTABLISH.confirm primitive.

9) Clause 8.2.1.1.1.2

Revise clause 8.2.1.1.1.2 as follows:

8.2.1.1.1.2 Actions at the destination AAL type 2 service endpoint

Upon receiving an indication from an incoming protocol entity instance requesting a new connection, the nodal function checks the availability of the CID value and other resources (e.g., indicated by the Transfer Capability parameter), in the incoming AAL type 2 path.

NOTE 1 – In case of interworking, the Transfer Capability and the Preferred Transfer Capability may be generated by the AAL type 2 service endpoint (see Annex C).

The following parameters – if they were conveyed by the incoming protocol entity instance – shall not be modified by the nodal function:

- the Destination Service Endpoint Address;
- the Origination Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the Transfer Capability;
- the Preferred Transfer Capability;
- the Transfer Capability Support;
- the Link Characteristics;
- the Preferred Link Characteristics;
- the Modify Support for Link Characteristics;
- the SSCS Information;
- the Preferred SSCS Information;
- the Modify Support for SSCS Information;
- the Path Type;
- ••
- the Connection Priority; and
- the Test Connection Indicator.

The following parameters – if they were conveyed by the incoming protocol entity instance – have significance to the served user only; therefore, they shall not be examined by the nodal function:

- the Origination Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the SSCS Information;
- the Preferred SSCS Information; and
- the Modify Support for SSCS Information.

If the Test Connection Indicator parameter is present, a "locally blocked" or "remotely blocked" AAL type 2 path shall be acceptable for the incoming connection.

If the CID and the other resources are available for the new connection, they are allocated to the new connection and then the AAL type 2 service endpoint address is examined. The nodal function determines that the destination AAL type 2 service endpoint has been reached.

When the nodal function checks the availability of resources in the incoming AAL type 2 path, the Connection Priority information, if received, is taken into consideration.

Under the normal condition, when the network is not congested and the AAL Type 2 service endpoint has the necessary resources to complete it, the connection establishment is processed without special treatments (see Notes in 8.2.1.1.1.1).

If a Temporary Alternative Routing (TAR) control parameter or a Hop Counter parameter is received, they shall be ignored.

AAL type 2 service endpoint internal resources are allocated for the new connection from the incoming AAL type 2 path to the destination AAL type 2 served user. The Connection Priority information, if received, is taken into consideration when allocating these resources.

The nodal function acknowledges the successful AAL type 2 connection establishment towards the incoming protocol entity instance. The nodal function shall pass the following parameters to the incoming protocol entity instance only if they were conveyed by the incoming protocol entity instance:

- the Transfer Capability Support;
- the Modify Support for Link Characteristics; and
- the Modify Support for SSCS Information.

An ESTABLISH.indication primitive is sent to the AAL type 2 served user to inform it of the successfully established new connection. The nodal function shall pass the following parameters to the destination AAL type 2 served user only if they were conveyed by the incoming protocol entity instance:

- the Origination AAL type 2 Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the Transfer Capability;
- the Preferred Transfer Capability;
- the Transfer Capability Support;
- the Link Characteristics;
- the Preferred Link Characteristics;
- the Modify Support for Link Characteristics;
- the SSCS Information;
- the Preferred SSCS Information;
- the Modify Support for SSCS Information;
- the Path Type;
- the Connection Priority; and
- the Test Connection Indicator.

NOTE 2 – Through-connection at AAL type 2 service endpoints is not specified by this Recommendation. It may be controlled by the AAL type 2 served user.

10) Clause 8.2.1.1.2.1

Revise clause 8.2.1.1.2.1 as follows:

8.2.1.1.2.1 Actions at the originating AAL type 2 service endpoint

If the AAL type 2 path selection or the allocation of a CID and other resources for the outgoing AAL type 2 link described in 8.2.1.1.1.1 fails, a RELEASE.confirm primitive is returned to the AAL type 2 served user with one of the following causes:

- "Unallocated (unassigned) number";
- "No route to destination";
- "No circuit/channel available";
- "Resource unavailable, unspecified";
- "Network out of order"; or
- "Temporary failure".

NOTE – Path selection failure may be due to the unavailability of an AAL type 2 path with the requested path type.

If AAL type 2 service endpoint internal resources are not available for the new connection, a RELEASE.confirm primitive is sent to the AAL type 2 served user with the cause "Switching equipment congestion".

If the AAL Type 2 service endpoint cannot complete a high priority connection establishment request even after application of the preferential treatment, a RELEASE.confirm primitive is sent to the AAL type 2 served user with the cause "Resource unavailable, unspecified".

Upon receiving a negative acknowledgement for the connection setup request from the outgoing protocol entity instance, all the resources associated with this AAL type 2 link are released and made available for new traffic. The association to the outgoing protocol entity instance is released.

Features that enable a further connection attempt, involving the selection of a different AAL type 2 path within the same route or of an alternative route, may be implemented. Such reattempts may use the CEID parameter returned in the Release Confirm (RLC) message and may select a different AAL type 2 path within the same route only. If the CEID parameter specifies an AAL Type 2 path with insufficient resources available for the connection attempt, no connection attempt is made on that path.

If no further connection attempt is made, the AAL type 2 service endpoint internal resources are released and a RELEASE.confirm primitive is sent to the AAL type 2 served user with the cause received from the outgoing protocol entity instance.

When an indication is received from the outgoing protocol entity that the establishment request has been rejected, and there has been a change in the level of congestion of the adjacent node, the routing tables in the nodal function shall be updated accordingly. The absence of an Automatic Congestion Control parameter indicates that there is no reported congestion in the adjacent node, whilst if the Automatic Congestion Control parameter is present it indicates whether congestion level 1 or 2 has been exceeded. After the routing tables have been updated, the Automatic Congestion Control parameter is discarded.

Upon receiving an indication from the outgoing protocol entity instance that a timer has expired, the association to the outgoing protocol entity instance is released and a reset procedure is started (see 8.2.1.2.1.1 case 3 a)). The AAL type 2 service endpoint internal resources are released. A RELEASE.confirm primitive is sent to the AAL type 2 served user with the cause received from the outgoing protocol entity instance, i.e., "Recovery on timer expiry".

11) Clause 8.2.1.1.2.2

Revise clause 8.2.1.1.2.2 as follows:

8.2.1.1.2.2 Actions at the destination AAL type 2 service endpoint

If resources on the incoming AAL type 2 path are not available, the nodal function requests the incoming protocol entity instance to reject the AAL type 2 connection with one of the following causes as applicable:

- "Resource unavailable, unspecified"; or
- "Requested circuit/channel not available".

If the nodal function detects that the destination is not reachable it may issue a redirection request by rejecting the AAL type 2 connection with the cause "No route to destination" and include an alternative AAL type 2 path identifier in a Connection Element Identifier parameter.

If the nodal function is aware that the SSCS parameters are not supported, it requests the incoming protocol entity instance to reject the AAL type 2 connection with the cause "AAL parameters cannot be supported".

The association between the nodal function entity and its incoming protocol entity instance is released.

If an AAL type 2 path is "locally blocked" and an indication from an incoming protocol entity instance of the request for a new connection other than a test connection is received, the following actions are taken:

1) The indication of the request for a new connection establishment is ignored and the incoming protocol entity instance is instructed to terminate and enter state "Idle"; the association with the incoming protocol entity instance is released and an ERROR.indication primitive with the CEID and the cause "Temporary failure" is sent to layer management.
2) The blocking procedure specified in 8.2.1.2.2.1 case b) is initiated for the AAL type 2 path on which the new connection was requested to be established.

If an AAL type 2 path is "remotely blocked" and an indication from an incoming protocol entity instance of the request for a new connection other than a test connection is received, the following actions are taken:

1) The AAL type 2 path is set to "remotely unblocked".

   NOTE – This procedure shall not be considered as the normal way to remove the "remotely blocked" condition.
2) The incoming connection establishment request is processed normally, i.e., as if the AAL type 2 path was not "remotely blocked" to begin with.

If AAL type 2 service endpoint internal resources are not available for the new connection, a negative acknowledgement for the connection setup request shall be returned to the incoming protocol entity instance with the cause "Switching equipment congestion". The resources allocated to the incoming AAL type 2 path are released and the association between the incoming protocol entity instance and the nodal function is released.

If the AAL Type 2 service endpoint cannot complete a high priority connection establishment request even after application of the preferential treatment, a negative acknowledgement for the connection setup request shall be returned to the incoming protocol entity instance with the cause "Resource unavailable, unspecified". The resources allocated to the incoming AAL type 2 path are released and the association between the incoming protocol entity instance and the nodal function is released.

Upon receiving an indication from an incoming protocol entity instance requesting a new connection and the connection request is to be rejected, the nodal function checks the level of congestion of the node. If either of the two congestion thresholds is exceeded, an Automatic Congestion Control parameter is passed to the protocol entity with the rejection indication. This parameter indicates the level of congestion (congestion level 1 or 2) to the adjacent AAL Type 2 node.

12) Clause 8.2.2.1.1

Revise clause 8.2.2.1.1 as follows:

8.2.2.1.1 Successful connection set up

Upon receiving notification from an incoming protocol entity instance requesting a new connection, the nodal function checks the availability of the CID value and other resources (e.g., indicated by Transfer Capability parameter), in the incoming AAL type 2 path.

NOTE 1 – In case of interworking, the Transfer Capability and the Preferred Transfer Capability may be generated by the AAL type 2 switch (see Annex C).

If the Test Connection Indicator parameter is present, "locally blocked" or "remotely blocked" AAL type 2 paths shall be acceptable for the incoming connection.

If the CID and the other resources are available for the incoming AAL type 2 link, the resources are allocated to the new connection.

If the Hop Counter is received, and the hop counter procedure is activated, the nodal functions shall decrement the Hop Counter value by 1. If the result is greater than 0, the nodal function shall pass the updated Hop Counter to the outgoing protocol entity instance when it is invoked. If the Hop Counter is received, and the hop counter procedure is not activated, the nodal functions shall pass the Hop Counter unmodified to the outgoing protocol entity instance when it is invoked.

NOTE 2 – If the result is 0, see 8.2.2.1.2.

The AAL type 2 service endpoint address is then examined. The nodal function determines that the AAL type 2 connection needs to be routed further to reach the destination AAL type 2 service endpoint and analyses the routing information. It selects a route with sufficient AAL type 2 path resources on a path with the requested path type (or network default if the path type is not specified) to the next AAL type 2 node. It then selects an AAL type 2 path from within the route which is able to accommodate the new connection.

NOTE 3 – Routing typically is based on:

- Addressing information;
- Transfer Capability;
- Test Connection Indicator;
- Requested Path Type;
- Automatic congestion control and the congestion level in the routing tables; and
- Temporary Alternative Routing (TAR) control (see ITU-T Rec. E.412 [17]).

When the nodal functions selects a route, the Connection Priority information, if received from the incoming protocol entity instance is used to select a route that has sufficient AAL type 2 path resources to the succeeding AAL type 2 node.

If the "TAR controlled connection" indication is received, the nodal functions shall not apply network management Temporary Alternative Routing (TAR) to the same connection.

If a Hop Counter is not received, and the hop counter procedure is activated, the nodal function shall pass the Hop Counter containing an initial count value to the outgoing protocol entity instance when it is invoked. The initial count value shall be provisioned by the network operator on a per AAL type 2 node basis (31 maximum).

AAL type 2 node internal resources are allocated for the new connection from the incoming AAL type 2 path to the outgoing AAL type 2 path. The Connection Priority _information, if received, is taken into consideration when allocating these resources.

Under the normal condition, when the network is not congested and the AAL Type 2 node has the necessary resources to complete it, the connection establishment is processed without special treatments.

NOTE 4 – In times of network congestion, when the AAL Type 2 node does not have sufficient resources to complete all of the incoming connection establishment requests, as one option, the AAL Type 2 node may give preferential treatments based on the priority level.

NOTE 5 – The preferential treatment should include access to reserved network resources, e.g.:

- the highest priority connections are given access to available network resources including the resources reserved for highest priority connections;
- the second highest priority connections are given access to available network resources including the resources reserved for the second highest priority connections, except for the resources reserved for the highest priority connections, and so on.

NOTE 6 – Allocation of reserved network resources to specific priority levels is implementation specific, and is not a subject for standardization.

On the selected outgoing AAL type 2 path, the CID and other resources (e.g., indicated by Transfer Capability, Link Characteristics, or SSCS information) are allocated for the outgoing AAL type 2 link. The handling of Transfer Capability, Link Characteristics, and SSCS information is specified in Annex C.

The following parameters – if they were conveyed by the incoming protocol entity instance – shall not be modified by the nodal function:

- the Destination Service Endpoint Address;
- the Origination Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the Transfer Capability;
- the Preferred Transfer Capability;
- the Transfer Capability Support;
- the Link Characteristics;
- the Preferred Link Characteristics;
- the Modify Support for Link Characteristics;
- the SSCS Information;
- the Preferred SSCS Information;
- the Modify Support for SSCS Information;
- the Path Type;
-
- the Connection Priority; and
- the Test Connection Indicator.

The following parameters – if they were conveyed by the incoming protocol entity instance – have significance to the served user only; therefore, they shall not be examined by the nodal function:

- the Origination Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the SSCS Information;
- the Preferred SSCS Information; and
- the Modify Support for SSCS Information.

An outgoing protocol entity instance is invoked and the following parameters are passed to it:

- the Destination AAL type 2 Service Endpoint Address;
- the AAL type 2 Path Identifier;
- a CID value; and
- the Transfer Capability.

The nodal function shall pass the following parameters to the outgoing protocol entity instance only if they were conveyed by the incoming protocol entity instance:

- the Origination AAL type 2 Service Endpoint Address;
- the Served User Generated Reference;
- the Served User Transport;
- the Preferred Transfer Capability;
- the Transfer Capability Support;
- the Link Characteristics;
- the Preferred Link Characteristics;
- the Modify Support for Link Characteristics;
- the SSCS Information;
- the Preferred SSCS Information;
- the Modify Support for SSCS Information;
- the Path Type;
- the Connection Priority; and
- the Test Connection Indicator.

A received "TAR controlled connection" indication shall be passed to the invoked outgoing protocol entity instance unchanged; alternatively, if the "TAR controlled connection" indication is not received and the nodal function applies network management Temporary Alternative Routing to the connection, the nodal function shall pass a "TAR controlled connection" parameter to the invoked outgoing protocol entity instance.

If the Hop Counter has been received or generated by the nodal function, it is passed to the invoked outgoing protocol entity instance.

Through-connection in both directions will then be completed.

After receiving an indication of the successful AAL type 2 connection setup from the outgoing protocol entity instance, the incoming protocol entity instance is informed of the successful AAL type 2 connection setup. If one or more of the parameters Transfer Capability Support, Modify Support for Link Characteristics, or Modify Support for SSCS Information parameter, was received from the outgoing protocol instance they shall be conveyed to the incoming protocol entity instance.

13) Clause 8.2.2.1.2

Revise clause 8.2.2.1.2 as follows:

8.2.2.1.2 Unsuccessful/abnormal connection set up

If resources on the incoming AAL type 2 path are not available, the nodal function requests the incoming protocol entity instance to reject the connection with one of the following causes as applicable:

- "Resource unavailable, unspecified"; or
- "Requested circuit/channel not available".

The association between the nodal function entity and its incoming protocol entity instance is released.

If an AAL type 2 path is "locally blocked" and an indication from an incoming protocol entity instance of the request for a new connection other than a test connection is received, the following actions are taken:

1) The indication of the request for a new connection establishment is ignored and the incoming protocol entity instance is instructed to terminate and enter state "Idle"; the association with the incoming protocol entity instance is released and an ERROR.indication primitive with the CEID and the cause "Temporary failure" is sent to layer management.
2) The blocking procedure specified in 8.2.1.2.2.1 case b) is initiated for the AAL type 2 path on which the new connection was requested to have been established.

If an AAL type 2 path is "remotely blocked" and an indication from an incoming protocol entity instance of the request for a new connection other than a test connection is received, the following actions are taken:

1) The AAL type 2 path is set to "remotely unblocked".

   NOTE 1 – This procedure shall not be considered as the normal way to remove the "remotely blocked" condition.
2) The incoming connection establishment request is processed normally, i.e., as if the AAL type 2 path was not "remotely blocked" to begin with.

If the Hop Counter is received, the nodal functions shall decrement the Hop Counter value by 1. If the result equals 0, the nodal function shall request the incoming protocol entity instance to reject the connection with cause value "exchange routing error". The association between the nodal function entity and its incoming protocol entity instance is released and all the resources associated with the incoming AAL type 2 link are released and made available for new traffic.

In all cases where the request from an incoming protocol entity instance to establish a new connection has to be rejected, the nodal function checks the level of congestion of the node. If either of the two congestion thresholds is exceeded, an Automatic Congestion Control parameter is passed to the protocol entity with the rejection indication. This parameter indicates the level of congestion (congestion level 1 or 2) to the adjacent AAL Type 2 node.

If AAL type 2 node internal resources are not available for the new connection, a negative acknowledgement for the connection setup request shall be returned to the incoming protocol entity instance with the cause "Switching equipment congestion". The resources allocated to the incoming AAL type 2 path are released and the association between the incoming protocol entity instance and the nodal function is released.

If the AAL Type 2 node cannot complete a high priority connection establishment request even after application of the preferential treatment, a negative acknowledgement for the connection setup request shall be returned to the incoming protocol entity instance with the cause "Resource unavailable, unspecified". The resources allocated to the incoming AAL type 2 path are released and the association between the incoming protocol entity instance and the nodal function is released.

If the AAL type 2 path selection or the allocation of a CID and other resources for the outgoing AAL type 2 link described in 8.2.2.1.1 fails, a negative acknowledgement for the connection setup request shall be returned to the incoming protocol entity instance with one of the following causes:

- "Unallocated (unassigned) number";
- "No route to destination";
- "No circuit/channel available";
- "Resource unavailable, unspecified";
- "Network out of order"; or
- "Temporary failure".

NOTE 2 – Path selection failure may be due to the unavailability of an AAL type 2 path with the requested path type.

The resources allocated to the preceding AAL type 2 path are released and the association between the incoming protocol entity instance and the nodal function is released.

Upon receiving a negative acknowledgement from the outgoing protocol entity instance, all resources associated with the outgoing AAL type 2 link are released and made available for new traffic. The association to the outgoing protocol entity instance is released.

Features that enable a further connection attempt, involving the selection of a different AAL type 2 path within the same route or of an alternative route, may be implemented. Such reattempts may use the CEID parameter returned in the Release Confirm (RLC) message and may select a different AAL type 2 path within the same route only. If the CEID parameter specifies an AAL Type 2 path with insufficient resources available for the connection attempt, no connection attempt is made on that path.

If no further connection attempt is made, the AAL type 2 node internal resources are released, the rejection of the connection establishment is forwarded to the incoming protocol entity instance with the cause received from the outgoing protocol entity instance; a Connection Element Identifier parameter possibly received in the Release Confirm (RLC) message is not forwarded to the incoming protocol entity instance. All the resources associated with the incoming AAL type 2 link are freed. The association to the incoming protocol entity instance is released.

When an indication is received from the outgoing protocol entity that the establishment request has been rejected, and there has been a change in the level of congestion of the adjacent node, the routing tables in the nodal function shall be updated accordingly. The absence of an Automatic Congestion Control parameter indicates that there is no reported congestion in the adjacent node, whilst if the Automatic Congestion Control parameter is present it indicates whether congestion level 1 or 2 has been exceeded. After the routing tables have been updated, the Automatic Congestion Control parameter is discarded.

Upon receiving an indication from the outgoing protocol entity instance that a timer has expired, the association to the outgoing protocol entity instance is released and a reset procedure is started (see 8.2.1.2.1.1 case 3 a)). The AAL type 2 node internal resources are released. The rejection of the connection establishment is forwarded to the incoming protocol entity instance with the cause received from the outgoing protocol entity instance (i.e., "Recovery on timer expiry") and all the resources associated with the incoming AAL type 2 link are released and made available for new traffic. The association to the incoming protocol entity instance is released.

14) Clause B.3

Revise clause B.3 as follows:

B.3 Coding of the compatibility information of the new parameters for CS-1 and CS-2 networks

To ensure backward compatibility with AAL type 2 nodes conforming only to ITU-T Recs Q.2630.1 [15] or Q.2630.2 [16], the parameter compatibility field of the new parameter shall be set as indicated in Table B.5.

Table B.5/Q.2630.3 – Coding of the parameter compatibility information

	8	7	6	5	4	3	2	1
	pass-on not possible				general action			
Parameter	res.	send notification indicator	instruction indicator		res.	send notification indicator	instruction indicator	
Origination AAL type 2 Service Endpoint Address (OA2AE) in ERQ message	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	
Connection Priority (CP) in ERQ message	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	
Congestion Level (CL) in REL or RLC message	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 1** discard parameter	
Hop Counter (HC) in ERQ message	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	
TAR Controlled Connection (TCC) in ERQ message	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	
Transfer Capability Support (TCS) in ERQ and ECF messages	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 1** discard parameter	
Fixed Bandwidth Transfer Capability (FBW) in ERQ and MOD messages	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	
Variable Bandwidth Stringent Transfer Capability (VBWS) in ERQ and MOD messages	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	
Variable Bandwidth Tolerant Transfer Capability (VBWT) in ERQ and MOD messages	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	

Table B.5/Q.2630.3 – Coding of the parameter compatibility information *(end)*

	8	7	6	5	4	3	2	1
	pass-on not possible				general action			
Parameter	res.	send notification indicator	instruction indicator		res.	send notification indicator	instruction indicator	
Preferred Fixed Bandwidth Transfer Capability (PFBW) in ERQ message	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	
Preferred Variable Bandwidth Stringent Transfer Capability (PVBWS) in ERQ message	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	
Preferred Variable Bandwidth Tolerant Transfer Capability (PVBWT) in ERQ message	**0**	**0** do not send notification	**0 1** discard parameter		**0**	**0** do not send notification	**0 0** pass on parameter	

Signalling for IEPS support in DSS2

ITU-T Rec. Q.2931 Amendment 5 (01/2006)

DIGITAL SUBSCRIBER SIGNALLING SYSTEM NO. 2 – USER-NETWORK INTERFACE (UNI) LAYER 3 SPECIFICATION FOR BASIC CALL/ CONNECTION CONTROL: SUPPORT FOR THE INTERNATIONAL EMERGENCY PREFERENCE SCHEME

Summary

ITU-T Rec. Q.2931 provides basic call and connection control for point-to-point connections in a B-ISDN. This amendment was produced to meet the need for the implementation of the International Emergency Preference Scheme (IEPS) as specified in ITU-T Rec. E.106. It contains the modifications to ITU-T Rec. Q.2931 (1995) in order to accommodate these needs. This amendment is designed to be compatible with implementations conforming to ITU-T Rec. Q.2931 (1995) and its Amendments 1, 2, 3 and 4.

1) Clause 1.3 – Capabilities supported by this Recommendation

Insert the following new capability:

15) IEPS

2) New clause 1.3.15 – IEPS

Add the following new clause:

1.3.15 IEPS

To support IEPS in the signalling protocol, a mechanism based on signalling an IEPS indicator is specified.

3) Clause 3.1.7 – Set-up

Add the following entry to Table 3-8:

Table 3-8/Q.2931 – SETUP message content

Information element	Reference	Direction	Type	Length
IEPS indicator	4.5	Both	O	4-5

4) Clause 3.2.7 – Set-up

Add the following entry to Table 3-19:

Table 3-19/Q.2931 – SETUP message content

Information element	Reference	Direction	Type	Length
IEPS indicator	4.5	Both	O	4-5

5) Clause 4.5.1 – Coding rules

Add the following entry to Table 4-3:

Table 4-3/Q.2931 – General information element format – Information element identifiers

Bits								
8	7	6	5	4	3	2	1	
1	0	0	1	1	0	0	0	IEPS indicator

6) New clause 4.5.26 – IEPS indicator

Add the following new clause:

4.5.26 IEPS indicator

The purpose of the IEPS indicator information element is to identify an IEPS call/connection for preferential call/connection set-up. It is optionally present in the SETUP message.

The IEPS indicator information element is coded as shown in Figure 4-36. The length of this information element is 5 octets.

8	7	6	5	4	3	2	1	Octet
IEPS indicator information element identifier								1
1	0	0	1	1	0	0	0	
ext. 1	Coding standard		IE instruction field Flag indicator	Res		IE action		2
Length of IEPS indicator contents								3 4
ext. 1	IEPS indicator							5

Figure 4-36/Q.2931 – IEPS indicator information element

Table 4-24/Q.2931 – IEPS indicator information element

IEPS indicator (octet 5)
Bits
7 6 5 4 3 2 1
0 0 0 0 0 0 0 No indication
0 0 0 0 0 0 1 IEPS marking for preferential call/connection set-up
Other values are spare.

7) New clause 5.10 – International Emergency Preference Scheme

Add the following new clause:

5.10 International Emergency Preference Scheme

5.10.1 Call/connection establishment at the originating interface

5.10.1.1 Call/connection request

When subscribed to, the DSS2 user entity will include the IEPS indicator IE in the SETUP message to provide preferential treatment for a call/connection. The call/connection is established with the IEPS indicator IE set as "IEPS marking for preferential call/connection set-up" in the SETUP message. Restrictive network management controls (e.g., DSS2 signalling congestion control procedure) are not applied to this call/connection.

5.10.1.2 Call/connection rejection

Procedures as specified in 5.1.8 apply.

5.10.2 Call/connection establishment at the destination interface

5.10.2.1 Incoming call/connection request

The network will map the IEPS call/connection marking transported through the network into the IEPS indicator information element and deliver it in the SETUP message to the DSS2 user entity. Restrictive network management controls (e.g., DSS2 signalling congestion control procedure) are not applied to this call/connection.

8) Clause J.2 – Abbreviations

Insert the following new abbreviation alphabetically:

IEPS International Emergency Preference Scheme

9) Clause J.3 – References

Insert the following new references:

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

[60] ITU-T Recommendation E.412 (2003), *Network management controls*.

[61] ITU-T Recommendation Q.1902.x series (2001), *Bearer Independent Call Control protocol Capability Set 2 (BICC CS2).*

[62] ITU-T Recommendation Q.1950 (2002), *Bearer independent call bearer control protocol*.

10) Appendix I – Guidelines for the use of Instruction indicators

Add the following entry to Table I.2:

Table I.2/Q.2931 – Typical use of Instruction indicators for the Q.2931 information elements which are related to the basic call control

Information elements	Flag	Origin	Action indicator
IEPS indicator	Not used	N&U	Not significant

Informative Supplement 53 to ITU-T Q-series Recommendations (09/2005)

SIGNALLING REQUIREMENTS TO SUPPORT THE INTERNATIONAL EMERGENCY PREFERENTIAL SCHEME (IEPS)

Summary

This Supplement is an information document intended to identify the signalling requirements required to support the International Emergency Preference Scheme (IEPS). IEPS is described in ITU-T Rec. E.106 and allows authorized users to have access to the International Telephone Service while the service is restricted due to damage, congestion, and/or other faults. IEPS capabilities provide authorized users with preferential call and connection handling.

1 Scope

This Supplement identifies the signalling requirements to support preferential capabilities within networks that are used to support emergency response/recovery activities and disaster responders. IEPS is described in ITU-T Rec. E.106, *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

2 References

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

[2] ITU-T Recommendation E.370 (2001), *Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks*.

[3] ITU-T Q-series Recommendations – Supplement 47 (2003), *Emergency services for IMT-2000 networks – Requirements for harmonization and convergence*.

[4] ITU-T Q-series Recommendations – Supplement 32 (2002), *Technical Report TRQ.2141.1: Signalling requirements for the support of narrowband services via broadband transport technologies – CS-2 signalling flows*.

[5] ITU-T Q-series Recommendations – Supplement 22 (1999), *Technical Report TRQ.3000: Operation of the bearer independent call control (BICC) protocol with digital subscriber signalling system No. 2 (DSS2)*.

[6] ITU-T Q-series Recommendations – Supplement 23 (1999), *Supplement to ITU-T Q.1901 Recommendation – Technical Report TRQ.3010: Operation of the bearer independent call control (BICC) protocol with AAL Type 2 Signalling Protocol (CS-1)*.

[7] ITU-T Recommendation Q.1902.x series (2001), *Bearer Independent Call Control protocol (Capability Set 2)*.

[8] ITU-T Recommendation Q.1950 (2002), *Bearer independent call bearer control protocol*.

[9] ITU-T Recommendation Q.2931 (1995), *Digital Subscriber Signalling System No. 2 – User-Network Interface (UNI) layer 3 specification for basic call/connection control*.

[10] ITU-T Recommendation Q.2630.3 (2003), *AAL type 2 signalling protocol – Capability Set 3*.

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

[12] ITU-T Recommendation M.3350 (2004), *TMN service management requirements for information interchange across the TMN X-interface to support provisioning of Emergency Telecommunication Service (ETS).*

3 Definitions

This Supplement defines the following term:

3.1 authenticating entity: A recognized entity that validates that the user of the IEPS is entitled to such use under the charter of that entity. There would be a number of such entities, each tasked with authenticating attempts for IEPS by their members.

4 Abbreviations and Acronyms

This Supplement uses the following abbreviations:

AAL 2	ATM Adaptation Layer type 2
ACC	Automatic Congestion Control
ACG	Automatic Code Gap
BICC CS-2	Bearer Independent Call Control protocol, Capability Set 2
B-ISDN	Broadband ISDN
B-ISUP	B-ISDN User Part
CANF	CANcel From
CANT	CANcel To
CBC	Call Bearer Control Protocol
CPC	Calling Party's Category
DSS2	Digital Subscriber Signalling System No. 2
IAM	Initial Address Message
IEPS	International Emergency Preference Scheme
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
NMC	Network Management Control
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service

All other relevant abbreviations are contained in the above references.

5 Introduction

Disaster situations can occur any time, any place, unexpectedly. These events often significantly damage the community infrastructure and severely disrupt daily living. Recovery requires rapid response by local authorities, immediate reaction from utility service providers, and support from medical, construction, fire, and police resources. Effective communications are essential to facilitate the myriad activities for coordinating lifesaving activities concurrent with re-establishing control in the disaster area. Following a disaster, immediate response operations focus on saving lives, protecting property, and meeting basic human needs.

When a disaster strikes, the public telecommunications infrastructure generally sustains damage, experiences excessive traffic loads, and is subject to external interference that may severely limit the ability for response and recovery activities to communicate. Therefore, special provisions to facilitate effective communications for the emergency activities are necessary. This includes priority establishment and processing of communications through the telecommunication resources that remain available. IEPS traffic needs to receive preferential use of the surviving capacity of the impacted network.

6 General requirements

The general requirements for IEPS are currently contained in ITU-T Rec. E.106 for Integrated Services Digital Networks (ISDN), Public Land Mobile Networks (PLMN), and Public Switched Telephone Networks (PSTN), irrespective of the bearer technology. Essential network features are identified as priority dial tone, priority call set up, including priority queuing schemes, and exemption from restrictive network management controls, such as call gapping.

The basic services E.106 addresses are voice and data. The growing emergence of integrated voice and data services of next generation telecommunication and mobile networks not only supports telephony but also provides a variety of enhanced modes of communication. These additional services can also be used for emergency communications and will enable emergency recovery operations to have a comprehensive menu of supporting communication capabilities.

In addition to the IEPS priority indication, the country/network of call origination and multiple levels of priority are required to be supported in the call control network based on bilateral agreement between administrations. Similarly, the IEPS priority indication is required to be supported in the bearer control network.

7 Detailed requirements

7.1 Identification of IEPS traffic and priority levels

Calls need to be marked to identify authorized IEPS users and the identification be maintained through to completion. Support for the IEPS call indicator is required for signalling, switching, and in bearer and traffic channels.

An IEPS priority indicator is generated in a network of the call originating country. The IEPS priority indicator is set independently from any other indicator or condition and is included in the very first signalling message of the call set up procedure, e.g., IAM. The Bearer Control Signalling Protocol shall, where possible, signal the IEPS priority indicator in the very first signalling message of the bearer setup procedure, e.g., SETUP, INVITE, etc. This will ensure that the Bearer Relay Nodes provide priority to Bearer setup with an IEPS indicator. The IEPS priority indication is retained in call and bearer control throughout the call duration.

Networks supporting IEPS use the Calling party's category and IEPS indicator values to trigger IEPS treatment. These values should be set prior to accessing the international network (for example, within the originating national network or at the outgoing international gateway).

Thirty-two levels of priority have been identified within ISUP and BICC. Priority levels are not used to provide preferential treatment for the call. The lowest numerical value signals the highest priority.

Incoming international gateway exchanges may be equipped to map priority level indications received in the context of incoming international IEPS calls to national priority levels required and applied in the terminating countries. In case that mapping is not implemented, priority level may be discarded, however the call shall continue to be treated as a priority call.

7.2 Security

Security protection is necessary to prevent unauthorized users from accessing scarce resources needed to support emergency operations. This includes such threats as spoofing, intrusion, and denial of service. IEPS calls should be protected against possible attempts to obstruct or otherwise impede the provision, operation and performance of the IEPS service.

Additional procedures concerning national issues should be considered, but are outside the scope of this Supplement.

7.3 Interworking

IEPS may be accessed or terminated via legacy national preference schemes or emergency services. International networks supporting IEPS should, at a minimum, transparently carry additional national information.

Gateways between domains using different preference mechanisms must be able to translate IEPS markings (i.e., IEPS CPC value) appropriately.

The following relationship exists between a national legacy and the IEPS priority scheme:

i) Priority or preference within the international systems does not necessarily guarantee priority in national telecommunications networks.

ii) Priority or preference within national systems does not necessarily guarantee priority in the international telecommunications networks.

iii) IP-to-PSTN gateways should use the IEPS CPC value to maintain the identification for priority/preference for calls established as IEPS as consistent with clauses i and ii.

iv) PSTN-to-IP gateways should have the capability to recognize the IEPS CPC value of an IEPS call, consistent with clauses i and ii, and mark packets in some way that maintains the identification for priority/preference treatment.

IEPS may be accessed or terminated via national preference schemes or emergency services. With regard to the priority rights, the following relationship between a national and the international emergency system (IEPS) is ensured:

- Priority in national systems does not include priority in IEPS. This is to avoid IEPS access by non-entitled users.
- IEPS priority always includes priority in national systems. This is necessary to ensure IEPS access via national preference systems.

7.4 IEPS treatment

When a node receives an IEPS call (i.e., the CPC value is "IEPS"), the call establishment proceeds with priority. The call is established with the CPC set as "IEPS" in the outgoing call set up message.

The IEPS priority indicator is conveyed across the international signalling network. The IEPS priority indication invokes preferential call handling in international transit exchanges, e.g., special routing capabilities.

The IEPS priority indication provides exemption from restrictive network management controls.

The network should try to reduce call set-up failures due to timer expirations caused by, for example, queuing delays for trunk allocation on congested routes.

The IEPS priority indication does not invoke pre-emption in the international network.

7.4.1 Queuing (ISUP) and polling (BICC)

For ISUP IEPS calls, if the above procedure fails to immediately find an outgoing circuit, the call is queued and shall take precedence over any other normal call attempts.

For BICC IEPS calls, if the above procedure fails to immediately find a bearer, the optional polling sequence described in Annex B applies.

7.4.2 Routing

The networks may use the IEPS marker for special routing to maintain an IEPS communication. Should the destination have "call forwarding" initiated, the network should then continue to reroute and process the communication session with the IEPS marker to the new destination. IEPS calls should be exempt from call restrictions to certain specific destinations (e.g., country codes or area codes), if activated.

7.4.3 Quality of Service (QoS)

The QoS for different modes of service for IEPS would typically be designated as the best available to ensure clear clean communications and conveyance of important information. However, when the telecommunication resources are experiencing severe stress, an allowable degradation of QoS could be acceptable. This could occur only when resources have become unavailable to the point that the network cannot support non-emergency traffic and sufficient bandwidth and resources are not available to support the normally acceptable QoS level for emergency traffic.

Rather than lose the ability to communicate, emergency operations need to continue to convey critical information, even if with difficulty. Any possibility of getting information through is better than none at all. The IEPS needs to continue operation when only "best effort" service is available. Therefore, a special or supplemental class of QoS for IEPS may be necessary to define the conditions and terms for allowable degradation of service.

7.4.4 Exemption from restrictive Network Management Controls (NMCs)

Restrictive network management controls are not applied to this call. There are several types of restrictive NMCs that could negatively affect IEPS calls.

Code controls block traffic to destination codes that are difficult or impossible to reach. This conserves network resources to serve traffic that has a better chance of completing. Code controls are most effective for controlling focused overloads, a condition characterized by a surge of traffic from other parts of the network to a single office or customer identified by a destination code. Two code controls have been developed. Code blocking controls a percentage of calls forwarded to a destination code. Call gapping regulates the maximum rate at which calls are forwarded to a destination code.

Calls are subject to any pre-hunt control that may be in effect on that trunk group. Trunk group controls include CANcel From (CANF), CANcel To (CANT), Skip, Dynamic Overload Control, and Selective Incoming Load Control. The last two controls provide Automatic Congestion Control (ACC) by responding to machine congestion messages and "hard-to-reach" information sent by SS7. Automatic Code Gap (ACG) is another SS7 control imposed that could negatively affect IEPS calls.

7.4.5 DSS2 interaction with BICC call control

This clause describes the IEPS information mapping between the BICC signalling entity and the DSS2 signalling entity. IEPS information mapping between the BICC signalling entity and DSS2 signalling entity via the CBC (vertical) interface is shown in Table 1.

Table 1 – Mapping of IEPS information

BICC signalling entity (Parameter)	DSS2 signalling entity (Information Element)
Calling party's category (IEPS call marking for preferential call set up)	IEPS indicator (IEPS marking for preferential call/connection set up)

7.4.6 AAL2 interaction with BICC call control

This clause describes the IEPS information mapping between the BICC signalling entity and the AAL2 signalling entity. IEPS information mapping between the BICC signalling entity and AAL2 signalling entity via the CBC (vertical) interface is shown in Table 2.

Table 2 – Mapping of IEPS Information

BICC signalling entity (Parameter)	AAL type 2 signalling entity (Parameter)
Calling party's category (IEPS call marking for preferential call set up)	IEPS indicator

8 Conclusion

Support for IEPS needs to be developed and integrated into current and future networks, regardless of the technology.

Annex A/Q.Sup53

Support of IEPS bearer level priority indicator in E.106

A.1 Backward backbone network establishment composite flow

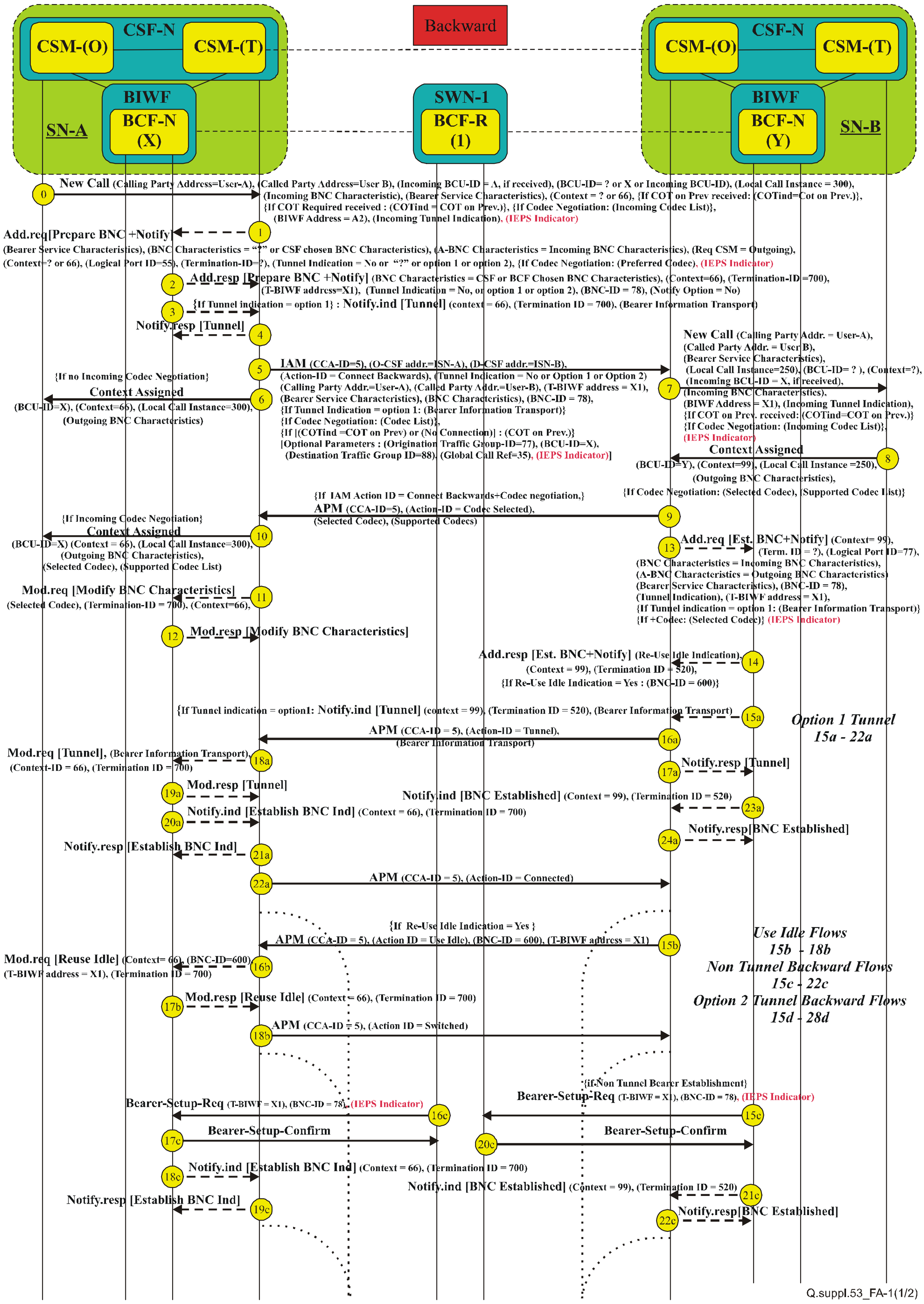


Figure A.1 (Part 1/2) – Composite backward connection establishment flow

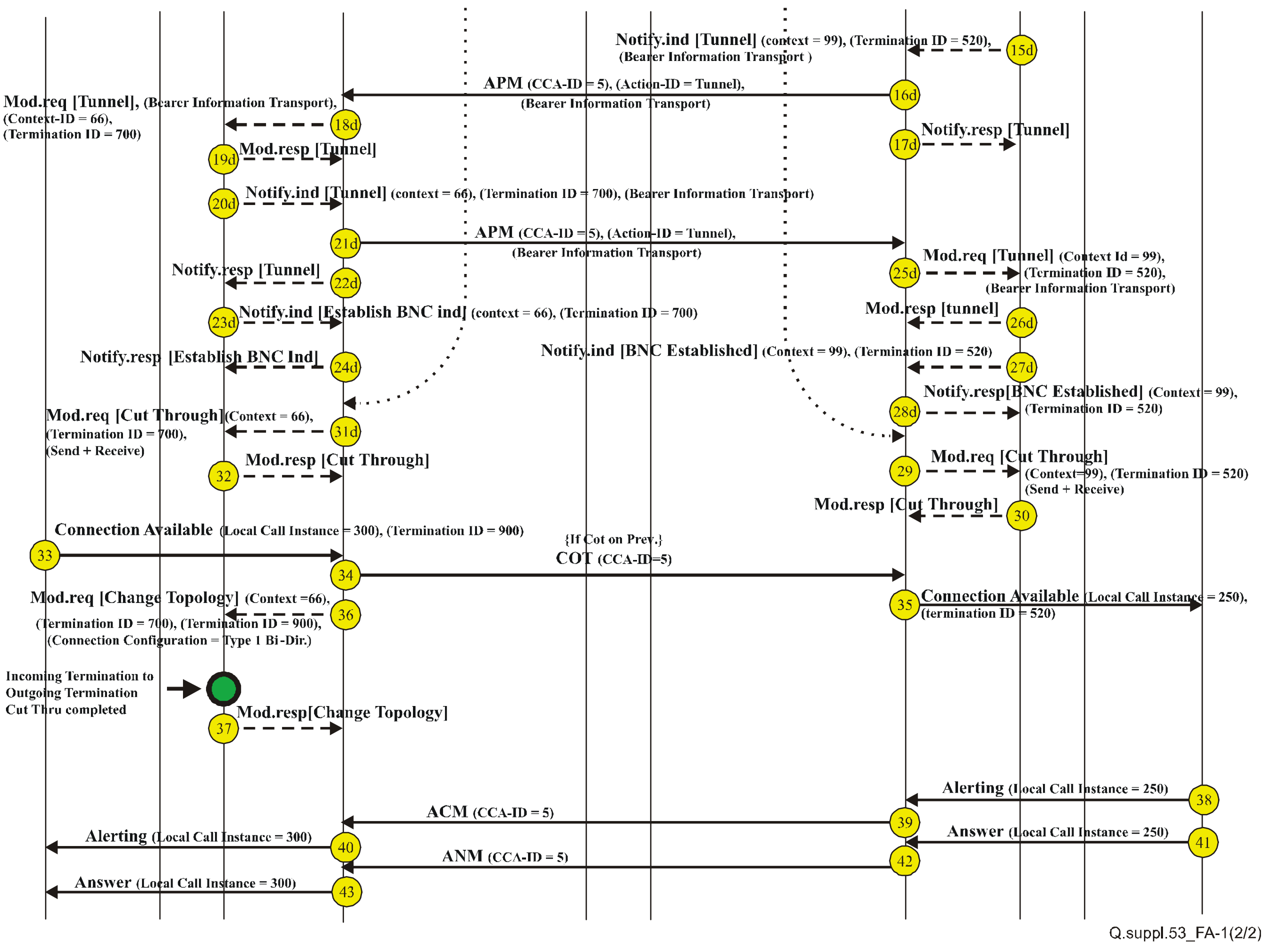


Figure A.1 (Part 2/2) – Composite backward connection establishment flow

The following numbered items describe the numbered flows shown above. Note that the following call flows are affected in support of IEPS: 0, 1, 5, 7, 13, 15c, and 16c.

0 New Call **SN-A:CSM-O to SN-A:CSM-T**

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS call (e.g. preferential treatment applied).

1 ADD.req (Prepare BNC with notification) **SN-A: CSM-T to BIWF-X**

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS connection (e.g. preferential treatment applied).

2 ADD.resp [BNC Prepared] BIWF-X to SN-A: CSM-T

As TRQ.2141.1.

3 Notify.ind [Tunnel] BIWF-X to SN-A: CSM-T

As TRQ.2141.1.

4 Notify.resp [Tunnel] SN-A: CSM-T to BIWF-X

As TRQ.2141.1.

5 IAM SN-A: CSM-T to SN-B: CSM-O

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS call (e.g. preferential treatment applied).

6 Context Assigned SN-A: CSM-T to SN-A: CSM-O

As TRQ.2141.1.

7 New Call SN-B: CSM-O to SN-B: CSM-T

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS call (e.g. preferential treatment applied).

Information Flows 8-12
As TRQ.2141.1

13 ADD.req (Est. BNC + Notify) SN-B: CSM-T to BIWF-Y

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS connection (e.g. preferential treatment applied).

Information Flows 14-18b

As TRQ.2141.1

15c Bearer-Setup.Req BIWF(Y) to SWN(1)

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS connection (e.g. preferential treatment applied).

16c Bearer-Setup.Req SWN(1) to BIWF(x)

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1 Resources are allocated for an IEPS connection (e.g. preferential treatment applied).

Information Flows 17c-43

As TRQ.2141.1

A.1.2 Forward backbone network establishment composite flow

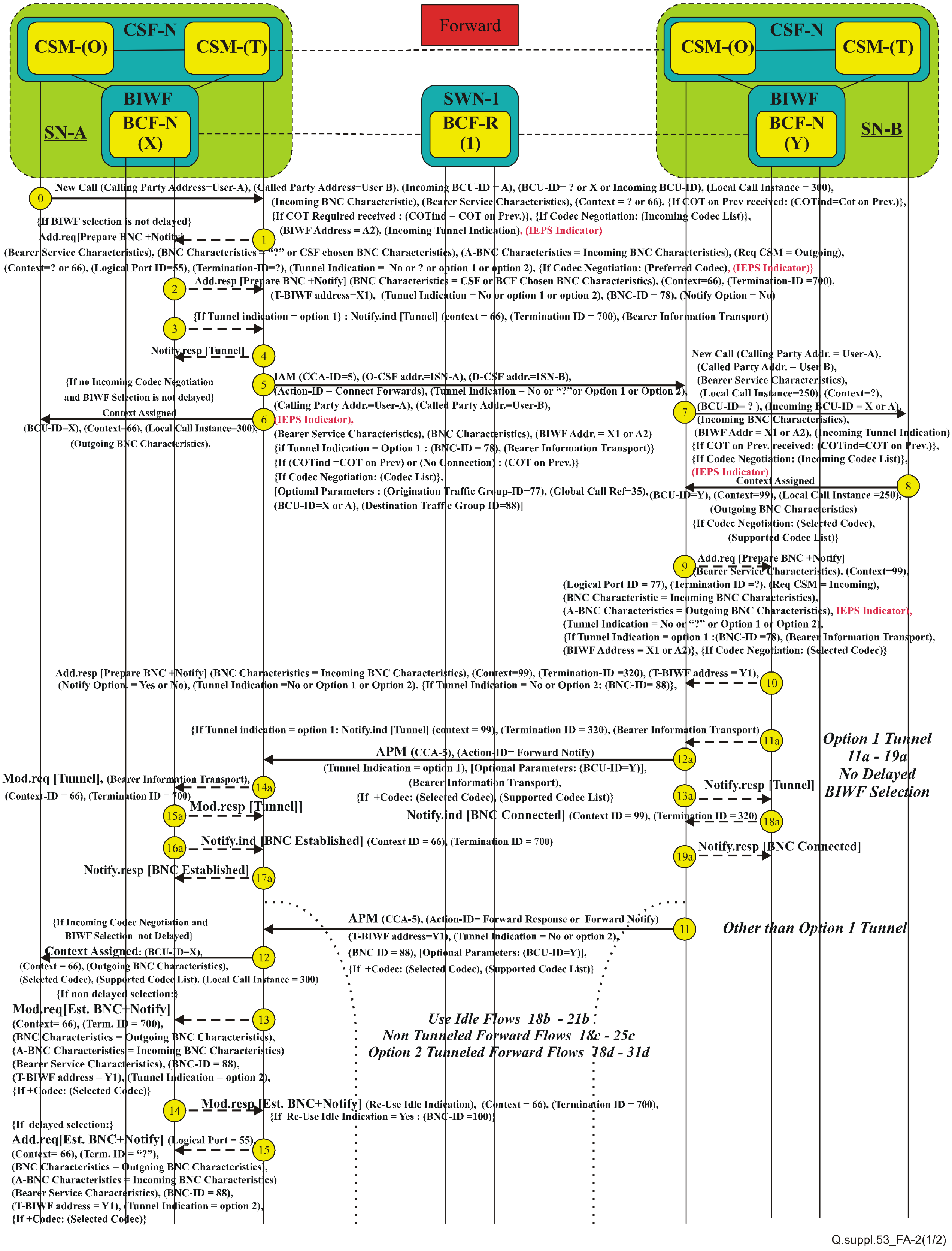


Figure A.2 (Part 1/2) – Composite forward establishment flow

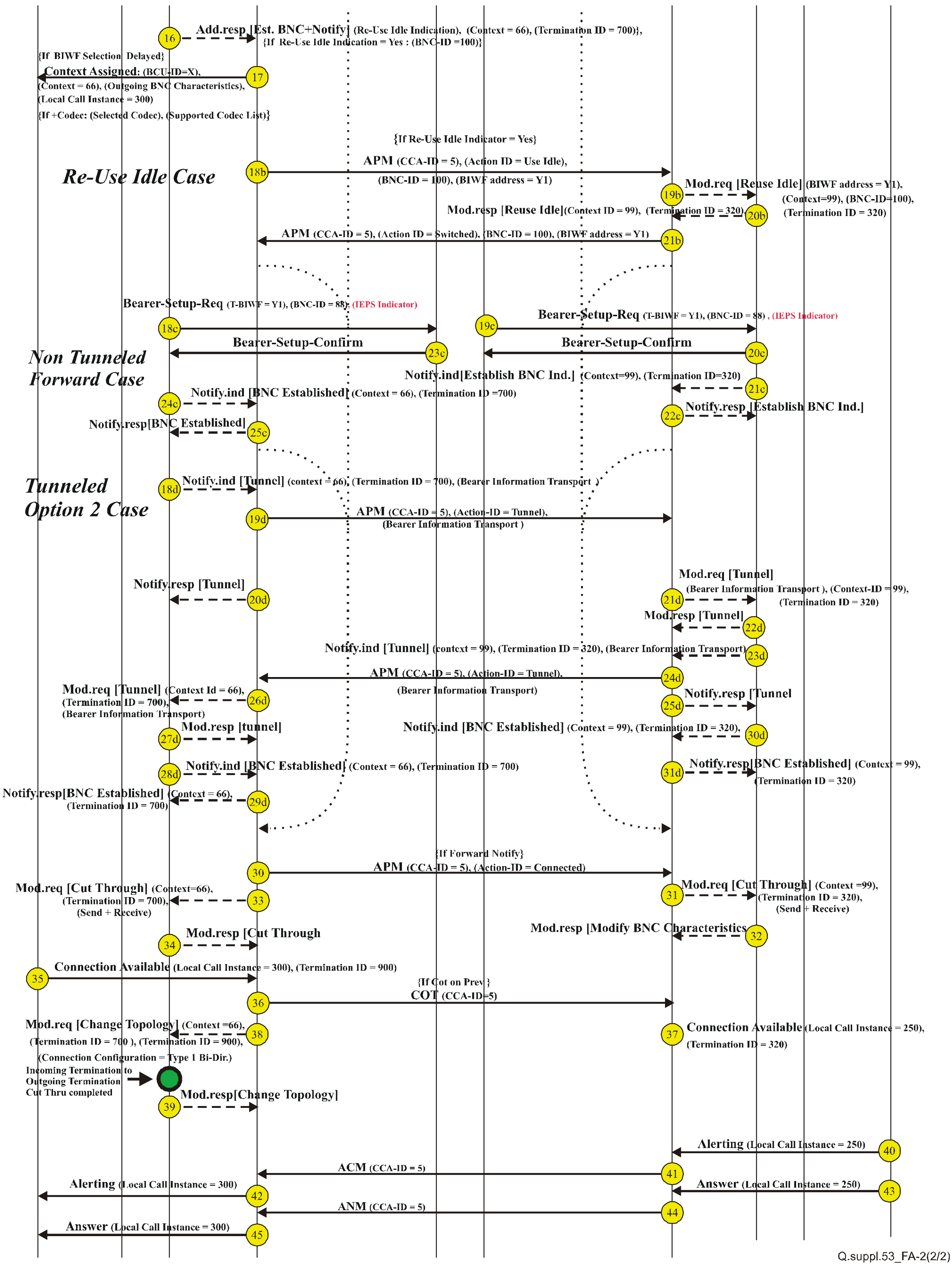


Figure A.2 (Part 2/2) – Composite forward establishment flow

The following numbered items describe the numbered flows shown above. Note the following call flows are affected in support of IEPS: 0, 1, 5, 7, 9, 18c, and 19c.

---

0 New Call **SN-A: CSM-O to SN-A: CSM-T**

Address Information	**Control information**	**Bearer information**
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS call (e.g. preferential treatment applied).

---

1 ADD.req (Prepare BNC with notification) **SN-A: CSM-T to BIWF-X**

Address Information	**Control information**	**Bearer information**
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS connection (e.g. preferential treatment applied).

---

2 ADD.resp [BNC Prepared] **BIWF-X to SN-A: CSM-T**

As TRQ.2141.1.

---

3 Notify.ind [Tunnel] **BIWF-X to SN-A: CSM-T**

As TRQ.2141.1.

---

4 Notify.resp [Tunnel] **SN-A: CSM-T to BIWF-X**

As TRQ.2141.1.

---

5 IAM **SN-A: CSM-T to SN-B: CSM-O**

Address Information	**Control information**	**Bearer information**
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS call (e.g. preferential treatment applied).

6 Context Assigned SN-A: CSM-T to SN-A: CSM-O

As TRQ.2141.1.

7 New Call SN-B: CSM-O to SN-B: CSM-T

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS call (e.g. preferential treatment applied).

8 Context Assigned SN-B: CSM-T to SN-B: CSM-O

As TRQ.2141.1.

9 ADD.req (Prepare BNC with notification) SN-B: CSM-O to BIWF-Y

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS connection (e.g. preferential treatment applied).

Information Flows 10-21b

As TRQ.2141.1

18c Bearer-Setup.Req BIWF(X) to SWN(1)

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS connection (e.g. preferential treatment applied).

19c Bearer-Setup.Req SWN(1) to BIWF(Y)

Address Information	Control information	Bearer information
As TRQ.2141.1	As TRQ.2141.1 IEPS Indicator	As TRQ.2141.1

Initiation of information flow: As TRQ.2141.1.

Processing upon receipt: As TRQ.2141.1. Resources are allocated for an IEPS connection (e.g. preferential treatment applied).

Information Flows 20c-45

As TRQ.2141.1

Annex B/Q.Sup53

Use of polling in the CSF for IEPS BICC calls

For BICC IEPS calls, the optional polling sequence for handling the seizure of a BIWF is:

1) The CSF shall attempt to seize a BIWF.

2) If there is no reply, or the BIWF indicates failure due to temporary resource unavailability, an ACM (no indication) is returned to the incoming side (unless COT is expected, in which case the ACM is sent once the COT has been received). A polling guard timer is started to prevent the CSF to be polling for an IEPS call for an excessive time.

3) The CSF may immediately select and attempt to seize a different BIWF. Upon failure due to temporary resource unavailability, or no reply, this step may be repeated to select other appropriate BIWFs.

4) If failure, due to temporary resource unavailability (or no reply), is indicated on all selected BIWFs, the CSF shall start a polling timer (Tpoll).

5) On expiry of Tpoll, the CSF shall attempt to seize the first BIWF. If there is no reply, or the BIWF indicates failure due to temporary resource unavailability, steps 3 and 4 are repeated until a BIWF indicates that resources are available. The time between the sets of BIWF seizure attempts (Tpoll) should increase for each successive set of seizure attempts.

A typical example sequence is illustrated in Figure B.1:

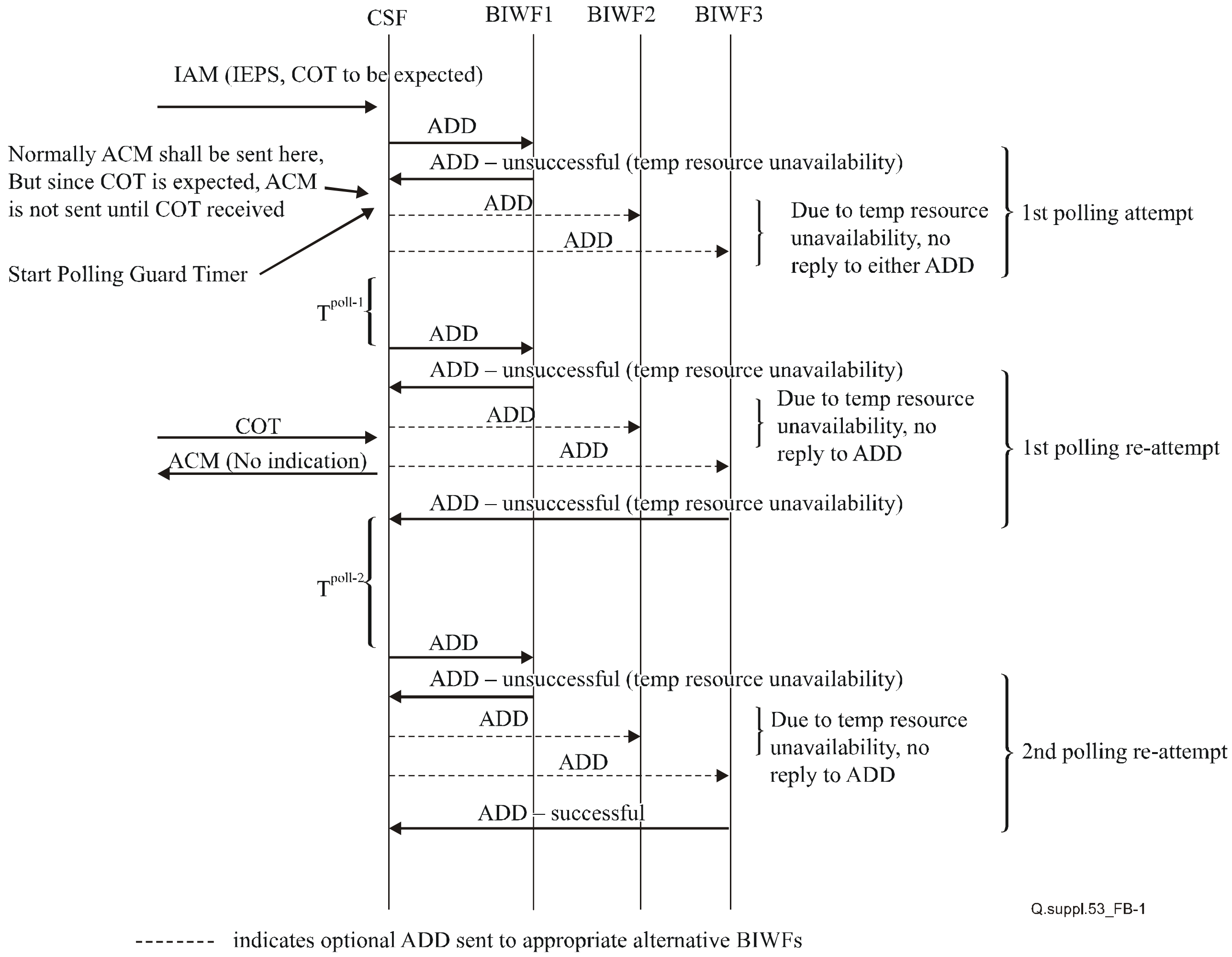


Figure B.1 – Example polling sequence in the CSF

31188

Printed in Switzerland
Geneva,- 2007
ISBN 92-61-12221-3