Internet Engineering Task Force Hal Folts
INTERNET DRAFT National Communications System
Expires November 15, 2000 May 15,2002

Requirements for Emergency Telecommunication Capabilities in the Internet.

draft-folts-ieprep-requirements-00.txt>

Status of This Memo

Copyright

Abstract: Priority telecommunication capabilities are required to support critical emergency communications through the public telecommunications infrastructure to support disaster recovery operations for saving lives and restoring community infrastructure. Many important issues are identified that are essential to ensuring effective emergency telecommunications capabilities are established in Internet-based infrastructures. The term "communication session" is used instead of "call" so that all modes of communication can be considered collectively; emergency telecommunication capabilities are not just limited to telephony traffic. No solutions are suggested, but the basic requirements are clearly identified for consideration by the ieprep Working Group of the IETF.

1. Introduction

Natural and man-made disasters can take place anywhere, anytime. These include, for example, earthquakes, floods, airplane crashes, and terrorist attacks. While some advance planning is possible for expected disaster events, most disasters happen unexpectedly.

Readily available telecommunication capabilities are essential for emergency recovery operations to quickly start saving lives and restoration of community infrastructure. A number of telecommunication facilities can be involved in disaster recovery operations. These include local mobile radio, dedicated satellite systems, transportable capabilities, and the public telecommunications infrastructure. Some of these facilities need to be deployed to the disaster site and may not be immediately available. The public telecommunication services, however, are generally at hand except in the most remote areas. The public capabilities include the traditional telephone network and the Internet, which can all be accessed via wire line, wireless, and various broadband facilities. Disaster recovery operations can significantly benefit from a variety of modes for interchange of critical information to organize and coordinate the emergency activities. Emergency voice communications have been supported today by a priority service through public telephone networks in some countries. Now, however, an evolution is taking place in traditional public telecommunication networks toward integrating circuit-switched and packet-based technologies. This promises to provide a rich menu of fully integrated capabilities for handling voice, message, data, and video traffic to greatly enhance disaster recovery operations.

Today mostly voice traffic using either VoIP or conventional telephony is used for emergency communications over wire line and wireless facilities. However, narrowband modes can also be applied, including instant messaging, Email, and telemedicine telemetry. In addition, wideband capabilities for video broadcast, conferencing, and telemedicine will also enhance emergency recovery operations.

During serious disaster events public networking facilities can experience severe stress due to damaged infrastructure and heavy traffic loads. As bandwidth gets severely constrained, it becomes difficult to establish and maintain effective communication sessions. It is essential that disaster recovery operations be given preferential use of remaining bandwidth. Authorized emergency communication sessions need to have priority use of available network resources over non-emergency traffic to quickly organize and coordinate saving of lives and restoration of community infrastructure.

Only people authorized by the appropriate authority are permitted to establish priority communication sessions through public networking facilities for facilitating immediate life-saving disaster recovery operations. Those typically authorized are local police, fire, and medical resources as well as designated government officials from local, regional, and national levels who will be responsible for various aspects of disaster recovery operations.

All emergency communication sessions will be processed as normal traffic along with all non-emergency traffic when sufficient network bandwidth and resources are available. ONLY when networks reach traffic saturation is there a need for giving emergency communication sessions preference over non-emergency communications. While this occurrence may never happen in the typical Internet-based environment, capabilities for preferential handling of emergency traffic need to be established in preparation for such a catastrophe.

The preferential capabilities for handling authorized emergency traffic should be accomplished using existing applications and standards when possible. Establishment of new and different standards would be both costly and unlikely to ever be implemented. The desired approach is to adopt existing standards and where needed adapt new standards with any necessary adjustments needed to support preferential treatment of emergency traffic during severe periods of congestion. The IETF needs to include consideration in the development of RFCs where there is potential benefit to fulfilling the requirements for preferential treatment of authorized emergency traffic through an Internet-based infrastructure.

2. Requirements

There are two areas that need to be addressed to provide the capabilities in an Internet-based environment to support handling of emergency traffic. The first is preferential processing of packet flows conveying emergency communications when the capacity of network resources becomes severely constrained. The second area is security, which includes authentication of authorized users originating emergency communication sessions and protection of emergency traffic from intrusion. The requirements and objectives to be considered and fulfilled wherever possible and practical to established effective capabilities for emergency communications are as follows:

A. Preferential Treatment - The objective is to enable emergency communication sessions to be processed preferentially during times of severe congestion and restricted bandwidth when the total traffic demand cannot be accommodated. Emergency communications need to be given priority over non-emergency communications under these severe conditions. When all traffic can be accommodated by the network resources, no preferential treatment is required.

   1) Access - Emergency communication sessions cannot be established until initial access is gained to the network.

Today there is not a ready provision for priority access to the public cellular and telephone systems. Access to the Internet via direct connection can normally interleave multiple sessions and therefore enable packets conveying emergency communications to share entry. A means for preferential access needs to be explored.

2) Establishment - Once access has been gained, the address of the destination as well as other parameters can be passed to enable establishment of the communication session. Once the initiating user is authenticated as being authorized to establish emergency communications in the telecommunications infrastructure, the established session can proceed and all packets need to covey an emergency identification and must receive preferential treatment over non-emergency packets.

3) Routing - In a connectionless infrastructure (Internet), packets are routed individually to the destination during an ongoing communication session. In a circuit-switched environment, once established via a single path, a communications session is essentially locked into place and needs no further priority processing. On the other hand, the additional consideration is needed for packet networks to continuing processing all packets supporting a specific instance of an emergency communication from initiation to completion.

4) Use of network resources - During a disaster event, the telecommunication facilities can experience damage that can severely limit the availability of resources to support the traffic demand. When this serious condition occurs, the emergency traffic needs to have precedence over non-emergency traffic. This may not occur often or ever, but if it does, it is particularly critical that emergency traffic gets preferential treatment over non-emergency traffic to facilitate saving of lives and restoration of community infrastructure.

5) Completion to destination - If a communication session cannot be completed in today's telecommunications environment either due to no answer or busy, the communication request in unsuccessful. In a single channel egress, a busy or no-answer condition prevents a session from reaching its destination. No-response is a dead-end, but busy destinations need to be overridden. When this is a packet interleave destination egress, the communication

should be delivered, but if it is a single point egress, a priority indication needs to be provided to the destination end, such as a priority "call waiting" alert.

B. Security - Two important considerations need to be taken into account for security issues for emergency communications. The first is to ensure rapid authentication of authorized users and then protection of emergency traffic from intrusion from outside interference.

1) Authentication - `Only users authorized by the appropriate national authority shall have access to the priority telecommunication capabilities in the pubic telecommunications infrastructure. In today's public telephone networks a credit-card process is used. This means entry of some 32 digits of information to complete establishment of a communication session. This is cumbersome and time-consuming. With future technology there is a need for a more time-responsive and streamlined mechanism for rapid authentication. New technology should be explored to seek an effective solution to this problem.

2) Intrusion - The overall problem of Internet security is being pursued by appropriate and expert resources in the IETF and elsewhere. However, the specific problem of

emergency traffic needs to be addressed. Emergency traffic needs to be protected against intrusion, spoofing, and specifically, denial of service. Emergency traffic must be processed without interference. If overall security measures that are established do not satisfy these specific requirements, additional consideration needs to be given to protection specifically focused on emergency traffic. While most emergency traffic for immediately organizing and coordinating local recovery operations, some emergency communications among certain government officials will need to be protected against eavesdropping and possibly against being traced to both source and destination points.

3. Example Scenarios

Some example instances for emergency communications are described below. These show some different levels of emergency communication requirements that need to be supported.

A. Local recovery operations - While mobile radio is the primary mode of communication for police and fire brigade operations, there is often a need to supplement these capabilities with access to the public telecommunication networks. This is particularly needed during the initial stages and immediately following the disaster event. These emergency communications can be accomplished through use of wireless, cellular phone or PDA, access where priority service may necessary due to congestion. Some mobile radio systems interface with public networks, but its use is often discouraged or avoided because of limited bandwidth availability. Communications outside the immediate local radio coverage area is often required to request additional resources from other areas and to notify and coordinate operations with regional (e.g. county and state) and national authorities.

B. Medical operations - The process of saving lives and getting victims to medical treatment, is greatly enhanced through the use of data telemetry to remotely provide victim vital signs to a central medical center. In addition, treatment of victims at the disaster site can be significantly accelerated through the use of video telemedicine transmissions to remote medical staff. These vital life-saving communications must have preferential treatment in the public telecommunications infrastructure.

C. Regional operations - The magnitude of the event may require recovery support from resources outside of the immediate area of impact. Critical information is provided for authorities to proclaim a disaster crisis and activate vital support resources. Regional emergency operations centers would the need immediate and effective telecommunication capabilities to rapidly organize and coordinate support from elsewhere regionally, nationally, or internationally.

D. National operations - The most serious disaster events can impact national security of a country. Therefore, immediate action is

required by government officials to organize and coordinate the highest level of emergency support resources. In addition with a serious threat to national security, actions to ensure continuity of government must be initiated. These types of activities need to not only have priority treatment for emergency communications in the public telecommunications domain, but they also require protection against eavesdropping of confidential/sensitive information. In addition, locations of source and destination of some critical national security traffic needs protection.

4. Conclusion

There are a number of critical issues that must be addressed by the IETF as outlined above. These are important ingredients to the total solution required for effective of an effective emergency telecommunication capabilities in the public telecommunication service infrastructure. Technical solutions are neither deliberately proposed nor suggested above to allow full consideration and innovation in seeking the effective solutions. There are many other aspects including the full systems, procedural, operational, policy, and regulatory aspects that also need to be address by other organizations. The IETF plays a critical role in this process to ensure that the technical capabilities in Internet-based infrastructures that support these requirements are established and sound.

5. Security Considerations

See draft-ietf-ieprep-security-00.txt on emergency telecom security.

6. Acknowledgements

Many thanks to Ian Brown and Ken Carlberg, for their comments on this draft.

8. Author's Address

Hal Folts, Senior Systems Engineer
Priority Services - Internet Team, Technology and Programs
National Communications System
foltsh@ncs.gov
+1 703 607-6186

9. Copyright "Copyright (C) The Internet Society (date). All Rights

FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PRUPOSE.