Network Working Group
Request for Comments: 4375
Category: Informational

K. Carlberg
G11

January 2006

Emergency Telecommunications Services (ETS) Requirements for a Single Administrative Domain

Status of This Memo

Copyright Notice

Abstract

This document presents a list of requirements in support of Emergency Telecommunications Service (ETS) within a single administrative domain. This document focuses on a specific set of administrative constraints and scope. Solutions to these requirements are not presented in this document.

1. Introduction

The objective of this document is to define a set of requirements that support ETS within a single domain. There have been a number of discussions in the IEPREP mailing list, as well as working group meetings, that have questioned the utility of a given mechanism to support ETS. Many have advocated over-provisioning, while others have favored specific schemas to provide a quantifiable measure of service. One constant in these discussions is that the administrative control of the resources plays a significant role in the effectiveness of any proposed solution. Specifically, if one administers a set of resources, a wide variety of approaches can be deployed upon that set. However, once the approach crosses an administrative boundary, its effectiveness comes into question, and at a minimum requires cooperation and trust from other administrative domains. To avoid this question, we constrain our scenario to the resources within a single domain.

The following provides an explanation of some key terms used in this document.

Resource: A resource can be a viewed from the general level as IP nodes such as a router or host as well as the physical media (e.g., fiber) used to connect them. A host can also be referred to in more specific terms as a client, server, or proxy. Resources can also be viewed more specifically in terms of the elements within a node (e.g., CPU, buffer, memory). However, this document shall focus its attention at the node level.

Domain: This term has been used in many ways. We constrain its usage in this document to the perspective of the network layer, and view it as being synonymous with an administrative domain. A domain may span large geographic regions and may consist of many types of physical subnetworks.

Administrative Domain: The collection of resources under the control of a single administrative authority. This authority establishes the design and operation of a set of resources (i.e., the network).

Transit Domain: This is an administrative domain used to forward traffic from one domain to another. An Internet Service Provider (ISP) is an example of a transit domain.

Stub Domain: This is an administrative domain that is either the source or the destination of a flow of IP packets. As a general rule, it does not forward traffic that is destined for other domains. The odd exception to this statement is the case of Mobile IP and its use of "dog-leg" routing to visiting hosts located in foreign networks. An enterprise network is an example of a stub domain.

1.1. Previous Work

A list of general requirements for support of ETS is presented in [RFC3689]. The document articulates requirements when considering the broad case of supporting ETS over the Internet. Since that document is not constrained to specific applications, administrative boundaries, or scenarios, the requirements contained within it tend to be quite general in their description and scope. This follows the philosophy behind its inception in that the general requirements are meant to be a baseline followed (if necessary) by more specific requirements that pertain to a more narrow scope.

The requirements presented below in Section 3 are representative of the more narrow scope of a single administrative domain. As in the case of [RFC3689], the requirements articulated in this document represent aspects to be taken into consideration when solutions are being designed, specified, and deployed. Key words such as "MUST",

"MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Scope

IETF standards that cover the resources within an administrative domain are within the scope of this document. This includes gateways, routers, servers, etc., that are located and administered within the domain. This document also does not restrict itself to a specific type of application such as Voice over IP.

Quality of Service (QoS) mechanisms are also within the scope of this document. These mechanisms may reside at the application, transport, or IP network layer. While QoS mechanisms may exist at the link/physical layer, this document only considers potential mappings of labels or code points.

Finally, since this document focuses on a single administrative domain, we do not make any further distinction between transit and stub domains within this document.

2.1. Out of Scope

Resources owned or operated by other administrative authorities are outside the scope of this document. One example is a SIP server that operates in other domains. Another example is an access link connecting the stub domain and its provider. Controlling only 1/2 of a link (the egress traffic from the stub) is considered insufficient for including inter-domain access links as a subject for this document.

3. Requirements

It must be understood that all of the following requirements pertain to mechanisms chosen by a domain’s administrative authority to specifically support ETS. If that authority chooses not to support ETS or if these mechanisms exist within the domain exclusively for a different purpose, then the associated requirement does not apply.

3.1. Label Mechanisms

Application or transport layer label mechanisms used for ETS MUST be extensible such that they can support more than one label. These mechanism MUST avoid a single off/on type of label (e.g., a single bit). In addition, designers of such a mechanism MUST assume that there may be more than one set of ETS users.

Network layer label mechanisms used for ETS SHOULD be extensible such that they can support more than one label. We make this distinction in requirements because there may be fewer bits (a smaller field) available at the network layer than in the transport or application layer.

3.2. Proxies

Proxies MAY set ETS labels on behalf of the source of a flow. This may involve removing labels that have been set by upstream node(s).

If proxies take such action, then the security measures discussed in [RFC3689] MUST be considered. More information about security in the single-domain context is found below in Section 5.

3.3. QoS mechanisms

[RFC3689] defines a label as an identifier, and the set of characteristics associated with the label as policy. However, QoS in the traditional sense of delay or bandwidth is not automatically bound to a label. MPLS [RFC3031] is an example of a labeling mechanism that can provide specific QoS or simply traffic engineering of labeled flows.

In the context of ETS, QoS mechanisms, at either the network or application layer, SHOULD be used when networks cannot be over-provisioned to satisfy high bursts of traffic load. Examples can involve bridging fiber networks to wireless subnetworks, or remote subnetworks connected over expensive bandwidth-constrained wide area links.

Note well. Over-provisioning is a normal cost-effective practice amongst network administrators/engineers. The amount of over-provisioning can be a topic of debate. More in-depth discussion on this topic is presented in the companion Framework document [FRAME].

3.4. Users

Regarding existing IETF-specified applications, augmentations in the form of labeling mechanisms to support ETS MUST NOT adversely affect its legacy usage by non-ETS users. With respect to future applications, such labeling mechanisms SHOULD allow the application to support a "normal" (non-emergency) condition.

3.5. Policy

Policy MUST be used to determine the percentage of resources of a mechanism used to support the various (ETS and non-ETS) users. Under certain conditions, this percentage MAY reach 100% for a specific set of users. However, we recommend that this "all-or-nothing" approach be considered with great care.

3.6. Discovery

There should be a means of forwarding ETS labeled flows to those mechanisms within the domain used to support ETS. Discovery mechanisms SHOULD be used to determine where ETS labeled flows (either data or control) are to be forwarded.

3.7. MIB

Management Information Bases (MIBs) SHOULD be defined for mechanisms specifically in place to support ETS. These MIBs MAY include objects representing accounting, policy, and authorization.

4. Issues

This section presents issues that arise in considering solutions for the requirements that have been defined for stub domains that support ETS. This section does not specify solutions nor is it to be confused with requirements. Subsequent documents that articulate a more specific set of requirements for a particular service may make a statement about the following issues.

4.1. Alternative Services

The form of the service provided to ETS users and articulated in the form of policies may be realized in one of several forms. Better than best effort is probably the service that most ETS users would expect when the communication system is stressed and overall quality has degraded. However, the concept of best available service should also be considered under such stressed conditions. Further, a measure of degraded service may also be desirable to ensure a measure of communication versus none. These services may be made available at the network or application layer.

4.2. Redundancy

The issue of making networks fault tolerant is important and yet not one that can be easily articulated in terms of requirements of protocols. Redundancy in connectivity and nodes (be it routers or servers) is probably the most common approach taken by network administrators, and it can be assumed that administrative domains apply this approach in various degrees to their own resources.

5. Security Considerations

This document recommends that readers review and follow the comments and requirements about security presented in [RFC3689]. Having said that, there tend to be many instances where intra-domain security is held at a lower standard (i.e., less stringent) that inter-domain security. For example, while administrators may allow telnet service between resources within an administrative domain, they would only allow SSH access from other domains.

The disparity in security policy can be problematic when domains offer services other than best effort for ETS users. Therefore, any support within a domain for ETS should be accompanied by a detailed security policy for users and administrators.

Given the "SHOULD" statement in Section 3.8 concerning MIBs, there are a number of related security considerations that need to be brought to attention to the reader. Specifically, the following:

- Most current deployments of Simple Network Management Protocol (SNMP) are of versions prior to SNMPv3, even though there are well-known security vulnerabilities in those versions of SNMP.

- SNMP versions prior to SNMPv3 cannot support cryptographic security mechanisms. Hence, any use of SNMP prior to version 3 to write or modify MIB objects do so in a non-secure manner. As a result, it may be best to constrain the use of these objects to read-only by MIB managers.

- Finally, any MIB defining writable objects should carefully consider the security implications of an SNMP compromise on the mechanism(s) being controlled by those writable MIB objects.

6. Acknowledgements

Thanks to Ran Atkinson, James Polk, Scott Bradner, Jon Peterson, and Ian Brown for comments on previous versions of this document.

7. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3689] Carlberg, K. and R. Atkinson, "General Requirements for Emergency Telecommunication Service (ETS)", RFC 3689, February 2004.

[FRAME] Carlberg, K., "A Framework for Supporting Emergency Telecommunications Services (ETS) Within a Single Administrative Domain", Work in Progress, December 2005.

Author’s Address

Ken Carlberg
G11
123a Versailles Circle
Baltimore, MD
USA

EMail: carlberg@g11.org.uk

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).