

ETS Requirements for Stub Domains
<[draft-carlberg-ets-req-stub-00.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#) [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt> The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

For potential updates to the above required-text see:
<http://www.ietf.org/ietf/1id-guidelines.txt>

Abstract

This document presents a list of requirements in support of Emergency Telecommunications Service (ETS) within a single administrative stub domain. This document is an extension of the General Requirements of [2] and focuses on a more 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 Stub 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 overprovisioning, while others have favored specific schemas to provide a quantifiable measure of service. One constant in these discussions is that the

Carlberg

Expires December 20, 2003

[Page 1]

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 & trust from other authoritative domains. To avoid this question, we constrain our scenario to the resources within a single stub domain.

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

Resource: A resource can be 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. As a 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 [2]. 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

Carlberg

Expires December 20, 2003

[Page 2]

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 stub domain. As in the case of [2], 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 [3].

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.

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 would only consider potential mappings of labels or code points.

2.1 Out of Scope:

Resources owned or operated by other administrative authorities are outside the scope of this document. One example are SIP servers that operate in other domains. Another example are access links 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.

Author's Note: it may be worthwhile to revisit the issue of access links. It is possible to constrain request emanating from the domain from an egress node (middle box or black box).

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).

3.3 QoS mechanisms

Quality of Service (QoS) mechanisms, at either the network or application layer, SHOULD be used when networks cannot be overprovisioned 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 overprovisioning can be a topic of debate. More indepth discussion on this topic is presented in the companion Framework document of [4].

3.4 Users

Any application layer label mechanisms used to support ETS MUST be capable of supporting both the set of ETS and non-ETS (presumably, normal) users.

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

Carlberg

Expires December 20, 2003

[Page 4]

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 MAY be used to determine where ETS labeled flows (either data or control) should be forwarded.

3.8 MIB

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

3.7 <Security?>

Author's note: Is it enough to rely on the requirements previously stated in [2]?

3.8 NAT/PAT

Author's Note: Should something be said here?

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 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 "Emergency"

The ITU has migrated away from the term "emergency" and ETS because of legal ramifications within the U.K. Apparently, there is a legal expectation when the term "emergency" is used as a service. Hence, the ITU is currently using the term Telecommunications for Disaster Relief (TDR). Legal issues such as this are outside the scope of this document and the IETF. However, to provide a bridge of understanding, the reader can assume that ETS within the IETF is synonymous with TDR in the ITU.

4.3 Redundancy

The issue of making network fault tolerant is important and yet not one that can be easily articulated in terms of requirements. 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 stub domains will apply this approach in various degrees.

5. Security Considerations

Security in terms of requirements is discussed [section 3](#).

6. Acknowledgements

Thanks to Ran Atkinson, James Polk, and Ian Brown for comments on an initial version of this draft.

7. References

- 1 Bradner, S., "The Internet Standards Process -- Revision 3", [BCP 9](#), [RFC 2026](#), October 1996.
- 2 Carlberg, K., Atkinson, R., "General System Requirements for Emergency Telecommunications Service", Internet Draft, Work In Progress, September, 2002
- 3 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.
- 4 Carlberg, K., "A Framework for Supporting ETS in Stub Domains", Internet Draft, Work in Progress, June 2003.

8. Author's Addresses

Ken Carlberg
G11
Gower Street
London, WC1E 6BT
United Kingdom
carlberg@g11.org.uk

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided as an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK 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 PURPOSE.

