Network Working Group
INTERNET-DRAFT

S.E. Hardcastle-Kille
ISODE Consortium

November 1992
Expires: June 1993

A simple profile for MHS use of Directory

Status of this Memo

This document is an Internet Draft. 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. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as a "working draft" or "work in progress."

Please check the I-D abstract listing contained in each Internet Draft directory to learn the current status of this or any other Internet Draft.

Abstract

The document "MHS Use of Directory to support MHS Routing" describes a comprehensive approach to MHS use of directory to support routing [HK92]. This document defines a strict subset of this document, which is intended to solve the most pressing problems. It also defines a practical first step for implementation, such that this subset can be deployed prior to fuller implementation.

This document does not repeat information in the other document. Duplication would only lead to the possibility of inconsistency.

WARNING: This document must be read in the contex of the document it profiles. It is meaningless as a standalone document.

This draft document will be submitted to the RFC editor as a protocol standard. Distribution of this memo is unlimited. Please send comments to the author or to the discussion group `<mhs-ds@mercury.udev.cdc.com>`.

1 Service Goals

The following goals are identified:

- No routing table configuration for simple MTAs in a PRMD (WEPs and gateways may do manual things).
- Single entry configuration for most sites.
- Do not replace function that is working reasonably well using existing approaches.
- Ignore issues which are not yet operational concerns. These can be handled by the full specification in due course.

2 Approach

The approach to routing is to use the single routing tree associated with the open community. MTAs will reference this tree. Simple MTAs need only do this, plus ad hoc configuration to route to a suitable MTA with a fuller manual configuration (e.g., a WEP). This document goes through section by section, referencing the full document, noting what support is needed.

3 Profile

3.1 General Table Handling

Support for subtrees, but not flat tables is needed.

3.2 O/R Address Hierarchy

Support for all attributes is needed, except:

mHSX121

mHSDomainDefinedAttribute

3.3 Local Addresses

This is supported.

3.4 MTA Naming

All MTAs are named within the O/R Address tree. The attributes which must be supported are:

responderAuthenticationRequirements

transportCommunity

remotePresentationAddress

3.5 Routing Trees

Only the single open community routing tree must be used. A variant on this profile might relax this restriction, perhaps to support a small number of routing trees. This relaxation should be noted in any statment referencing this specification.

3.6 Routing Information

The following attributes are used:

- authoritativeAddress
- mTAInfo

Routing action is always the default.

3.7 Indirect Connectivity

This is not used.

3.8 Protocol Mismatches

The transport community approach is used.

3.9 Supported Protocols

This approach is used, but only P1(88) and P1(84) are considered.

3.10 Capability Restrictions

These are not handled.

3.11 Pulling Messages

This is not done.

3.12 Authentication

For 1988 usage, the distinguished name is used to identify the remote MTA. Authentication will be by network address. Password will always be ASN.1 NULL.

For 1984 usage, no authentication is done.

The attribute must be supported, but only the `responderAuthenticationRequirements` attribute is used. For MTAs following this specification, the following values must be set if `bilateral-agreement-needed` is false.

mta-name-present true

aet-present true

aet-valid true

network-address true

simple-authentication false

strong-authentication false

If `bilateral-agreement-needed` is true, there are no restrictions on value. Where a WEP uses this scheme, information on the bilateral agreement will be determined locally (by private means).

The remotePresentationAddress attribute will always be present.

3.13 Policy

Policy will not be used.

3.14 Protocol Extensions

These will not be used.

3.15 Format Conversion

All issues relating to format conversion will be ignored.

3.16 RFC 822 Support

There is no support for RFC 822 or RFC 822/X.400 mappings by use of directory.

3.17 Distribution Lists

This will not be supported.

3.18 Redirects

Not supported.

3.19 Bad Addresses

The mechanisms will not be supported.

References

[HK92] S.E. Hardcastle-Kille. MHS use of the directory to support MHS routing, April 1992. Internet Draft.

4 Security Considerations

Security considerations are not discussed in this INTERNET–DRAFT .

5 Author's Address

Steve Hardcastle-Kille
ISODE Consortium
PO Box 505
London
SW11 1DX
England

Phone: +44-71-223-4062

EMail: S.Kille@ISODE.COM

DN: CN=Steve Hardcastle-Kille,
O=ISODE Consortium, C=GB

UFN: S. Hardcastle-Kille, ISODE Consortium, GB