

Network Working Group	M. Andrews	
Internet-Draft	ISC	
Expires: January 31, 2011	July 30, 2010	

[TOC](#)

Multi Match Label

draft-andrews-dnsexst-multi-match-label-00

Abstract

Idn users have expressed a need to have multiple labels be treated as one in the DNS. This document presents a method to do this by defining a new label type that ties a set of labels together that need to be treated indentially.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on January 31, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- 1. Introduction
- 2. Wire Format
- 3. Master File Format
- 4. Signaling client support for MML
- 5. Interaction with DNSSEC
- 6. Interaction with non MML parent zones
- 7. Interaction with non MML child zones
- 8. IANA Considerations
- 9. Security Considerations
- § Author's Address

1. Introduction

[TOC](#)

Multi Match Labels (MML) are intended to be used in owner names of records in the DNS to combine RFC 1035 labels that should be treated identically in a zone.

2. Wire Format

[TOC](#)

The MML has label type {TBD}. Following the label type there is a count of the number of sub labels, upto 255, (Note we could reduce this below 63 and encode in the first octet) followed by a series of RFC 1035 sub labels that make up the MML.

```

                                1 1 1 1 1 1
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      TBD              |      COUNT              |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      LEN              |                          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+
/              SUB LABEL              /
|                          +---+---+---+---+---+---+---+
|                          |      LEN              |
+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                          |                          |
/              SUB LABEL              /
/                          /
+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

When used in a domain name, MMLs extend the maximum length of a domain name to 1024 octets with the restriction that all domain names constructed using the MML are still restricted to 255 octets. This makes the effective length of the MML be the length of the longest sub label in the MML.

3. Master File Format

[TOC](#)

[To be fully described].
e.g. {sublabel1,sublabel2,sublabel3}

4. Signaling client support for MML

[TOC](#)

Client side support for MML support is signaled using EDNS version 1. Clients that do not signal that they support MML labels will receive the RFC 1035 sub labels that match the query name.

5. Interaction with DNSSEC

[TOC](#)

The canonical format of a MML is the MML with each sub label in canonical format as per RFC 4035. Zones that use MML labels need to use DNSSEC algorithm types that signal the potential use of MML. MML zones are treated as insecure by validators that are not MML aware. NSEC and NSEC3 chains are constructed as if all of the combinations of names in owner name exists separately for all MMLs within the zone. MMLs within the zone name are NOT expanded but are kept as MMLs. This permits name error (NXDOMAIN) to be returned. If the zone name contains MMLs the signer name and be any of the RFC 1035 names the MML maps to.

6. Interaction with non MML parent zones

[TOC](#)

The parent zone delegates each of the zone names that makes up the names in the MML named zone.

[TOC](#)

7. Interaction with non MML child zones

The child server implements all of the potential zones names.

8. IANA Considerations

[TOC](#)

TBD

9. Security Considerations

[TOC](#)

TBD

Author's Address

[TOC](#)

	Mark P. Andrews
	Internet Systems Consortium
	950 Charter Street
	Redwood City, CA 94063
	US
Email:	marka@isc.org