Internet Draft
Document: draft-fecyk-dmp-02.txt
Expires: November 2004

G. Fecyk
Pan-Am Internet Services

May 2004

Designated Mailers Protocol

Status of this Memo

Abstract

This document describes the Designated Mailers Protocol (DMP); a proposal for identifying computer systems authorized to act as Simple Mail Transfer Protocol (SMTP) clients for an e-mail domain.

Conventions used in this document

"Client" refers to a host creating a network session with a server. Clients may also be servers in real implementations. "Server" refers to a host accepting a network session from a client as defined above.

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

"Domain" refers to both a domain in the RFC 1034 sense [RFC 1034] and in the portion of an e-mail address after the "@" sign.

In examples, clients act on behalf of the fictitious domain "example.com" or "example.org". Servers act on behalf of the fictitious domain "example.net". Internet Protocol v4 address examples come from the non-routable network 192.0.2.0/24.

Example records use the format described in RFC 1034 section 3.6.1. The $ORIGIN keyword is used to shorten example record names. This example describes "recordname.example.com." as two lines:

```
$ORIGIN example.com.
recordname TXT "this is a test"
```

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

Table of Contents

1. Introduction

NOTE: This document is part of the Lightweight Mail Authentication Protocol work of the Anti-Spam Research Group (ASRG) of the Internet Research Task Force.

Designated Mailers Protocol is a proposal to identify computers authorized to act as Simple Mail Transfer Protocol (SMTP) [RFC 2821] clients in the name of a domain. Mail Transfer Agents (MTAs) that look up DMP records may refuse mail from sources not identified in DMP records. This reduces the amount of "spoofed" mail the MTA accepts in the name of a domain.

A domain publishes DMP records in the Domain Name System (DNS) [RFC 1034]. This ensures control remains with the domain's administrators, and allows the MTA using DMP to take advantage of DNS record caching to reduce the amount of network overhead that DMP queries require. DMP uses the TXT Resource Record type, which works without modifying existing DNS software.

DMP does not rely on any DNS records other than the DMP records themselves, nor does it rely on information stored in the e-mail body, including headers. This avoids problems identifying SMTP clients by Address (A), Mail Exchange (MX) or Pointer (PTR) records

where the sending domain's administrators may not have control over them. This also avoids blocking otherwise useful functionality of SMTP, such as sending mail on behalf of another user.

DMP is an OPTIONAL extension to SMTP. DMP supports Extended SMTP (ESMTP) and supports all SMTP functionality, including forwarding,

delivery status notifications, and so on, while providing a domain with this control.

2. The Argument for Authenticating Incoming E-mail by Domain

Junk e-mailers routinely falsify sender envelopes in order to misdirect complaints about their junk e-mail, resulting in an industry consisting of users who fake mail for fun and profit.

Authors of viruses that propagate via e-mail falsify sender envelopes to hide the origins of the virus-infected computers.

Confidence artists, posing as members of popular domains, routinely attempt to obtain confidential information from unsuspecting victims.

Designated Mailers Protocol reduces the impact of "spoofing" the source of an e-mail message. DMP is not as strong as cryptographic based authentication, but it is easier to implement and does not require dramatic changes to e-mail software.

DMP does not prevent e-mail with solely a falsified mailbox name, but it allows the administrators of a domain to audit such e-mail, by ensuring only its own computers may send mail on behalf of the domain.

3. Changes Since Last Revision

The format of DMP records used since the last Internet-Draft (draft-fecyk-dsprotocol-04.txt) has not changed.

DMP now incorporates design elements of the Designated Relays Inquiry Protocol, a work-in-progress by Raymond S Brand and others (See Contributors section). Notably, DMP provides for a second tier of inspection, permitting e-mail forwarded through certain types of mail forwarding protocols. Receiving domain administrators may choose any combination of outcomes based on the DMP query results.

The -01 revision corrects grammatical problems and clarifies some of the wording.

The 02 revision contains minor corrections to examples to match the provided flowchart, and includes an IRTF notice in the Introduction.

4. DMP Record Format and Designating SMTP Clients

DMP records of a domain MUST appear in a sub-domain "_smtp-client". From there, records MUST appear in sub-domains identified by protocol type, such as "in-addr" for IPv4 and "ip6" for IPv6. Further sub-domains will appear because of designating hosts and networks as allowed to send e-mail on behalf of the sender's domain.

DMP records use the TXT Resource Record type. All DNS software supports this record type and it may store arbitrary values. DMP uses the format defined in [RFC 1464]. An algorithm that looks up RFC 1464 style records MAY be used but is NOT REQUIRED.

A participating domain MUST publish these minimum records.

```
; REQUIRED: DMP Participant Identifier
_smtp-client.$DOMAINNAME. TXT "dmp="
; RECOMMENDED: Default DMP response for servers supporting wildcards
*._smtp-client.$DOMAINNAME. TXT "dmp=deny"
```

The first record identifies the domain, $DOMAINNAME, as a participant with its own designated mailer hosts. The second is a RECOMMENDED record that provides a default response to queries. If there are no additional DMP records, the domain effectively publicizes that they do not send SMTP traffic.

A participating domain sending SMTP traffic MUST publish one or more additional records identifying the networks or network addresses permitted to send SMTP traffic for their domain.

```
$REV-ADDRESS.$ADDRESS-TYPE._smtp-client.$DOMAINNAME. TXT "dmp=allow"
```

$REV-ADDRESS is the host or network's address represented in reverse form, as used in in-addr.arpa or ip6.arpa. $ADDRESS-TYPE is the type of address, such as "in-addr" for IPv4 or "ip6" for IPv6. DMP supports any network protocol that supports address-to-name mapping in the DNS.

DMP uses the keywords "allow" and "deny" for their English meanings. Record contents are case-insensitive, so "DMP=ALLOW" means the same as "dmp=allow".

DMP records MAY use wildcards, if the DNS server software supports them, to publish fewer records, publish records for sub-domains, or for other purposes. As not all DNS software supports wildcards, or may handle wildcards differently, wildcards are NOT REQUIRED.

Domains publishing DMP records MUST also publish DMP records for each sending host's Fully Qualified Domain Name (FQDN). This identifies the host as being permitted to send mail with null reverse paths (MAIL FROM:<>) and also being permitted to forward

mail, where the sender's domain may not otherwise designate this host.

```
; REQUIRED: Default DMP record for hosts
_smtp-client.$FQDN. TXT "dmp="
; REQUIRED: One or more DMP records identifying the host's network address or addresses
$REV-ADDRESS-1.$ADDRESS-TYPE._smtp-client.$FQDN. TXT "dmp=allow"
$REV-ADDRESS-2.$ADDRESS-TYPE._smtp-client.$FQDN. TXT "dmp=allow"
; [...]
$REV-ADDRESS-N.$ADDRESS-TYPE._smtp-client.$FQDN. TXT "dmp=allow"
; RECOMMENDED: Default DMP lookup result
*._smtp-client.$FQDN. TXT "dmp=deny"
```

4.1 Example DMP Records by Internet Protocol v4 Address

The domain example.com designates two IPv4 addresses as allowed to send mail for example.com:

```
$ORIGIN example.com.
_smtp-client TXT "dmp="
*._smtp-client TXT "dmp=deny"
1.2.0.192.in-addr._smtp-client TXT "dmp=allow"
2.2.0.192.in-addr._smtp-client TXT "dmp=allow"
```

The domain example.com designates the IPv4 network 192.0.2.0/24 as allowed to send mail for example.com:

```
$ORIGIN example.com.
_smtp-client TXT "dmp="
*._smtp-client TXT "dmp=deny"
*.2.0.192.in-addr._smtp-client TXT "dmp=allow"
```

The host sender.example.com designates its IPv4 address at 192.0.2.1:

```
$ORIGIN example.com.
_smtp-client.sender TXT "dmp="
*._smtp-client.sender TXT "dmp=deny"
1.2.0.192.in-addr._smtp-client.sender TXT "dmp=allow"
```

4.2 Example DMP Records by Internet Protocol v6 Address

The domain example.com designates two IPv6 addresses as allowed to send mail for example.com:

```
$ORIGIN example.com.
_smtp-client TXT "dmp="
*._smtp-client TXT "dmp=deny"
```

```
0.F.E.D.C.B.A.9.8.7.6.5.4.3.2.1.1.0.0.0.1.1.A.C.1.C.0.0.5.4.3.2.ip6.
_smtp-client TXT "dmp=allow"
1.F.E.D.C.B.A.9.8.7.6.5.4.3.2.1.1.0.0.0.1.1.A.C.1.C.0.0.5.4.3.2.ip6.
_smtp-client TXT "dmp=allow"
```

The host sender.example.com designates its own IPv6 address 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0:

```
$ORIGIN example.com.
_smtp-client.sender TXT "dmp="
*._smtp-client.sender TXT "dmp=deny"
0.F.E.D.C.B.A.9.8.7.6.5.4.3.2.1.1.0.0.0.1.1.A.C.1.C.0.0.5.4.3.2.ip6.
_smtp-client.sender TXT "dmp=allow"
```

5. Querying for DMP Records and Recommended Actions

A server looking up DMP records queries on the following information provided by the client:

- Connecting network address and Domain part of the sender envelope (MAIL FROM:<>) or
- Connecting network address and HELO or EHLO identifier. The HELO or EHLO identifier MUST be the client host's Fully Qualified Domain Name (FQDN).

The layout of the DMP records allows the server to query the address and domain or FQDN with a single DNS query. The result will be one of four possibilities:

- A successful query, and one or more returned TXT records, at least one of which will contain the string "dmp=allow", meaning this client is permitted to send mail on behalf of this domain or FQDN,
- A successful query, and one or more returned TXT records, at least one of which will contain the string "dmp=deny", meaning this client is NOT permitted to send mail on behalf of this domain or FQDN,
- A query that returns NXDOMAIN, or a query that returns no DMP records or multiple and conflicting DMP records (such as two TXT records, one reading "dmp=allow" and one reading "dmp=deny"), indicating this client does not have a valid DMP record in the

  domain or FQDN, or
. A query that returns SERVFAIL, indicating a temporary error.

A server MAY perform an additional query to determine if a domain or FQDN participates in DMP. The result will be one of three possibilities:

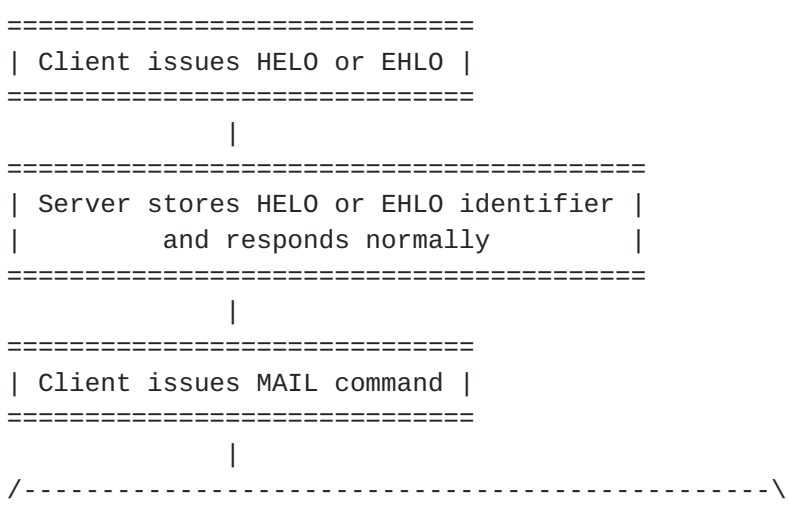
. A successful query, and one or more returned TXT records, one or more of which will contain only the string "dmp=", indicating this domain or FQDN participates in DMP,
. A query that returns NXDOMAIN, or a query that returns no "dmp=" record, indicating the domain does not participate in DMP, or has invalid DMP records, or,
. A query that returns SERVFAIL, indicating a temporary error.

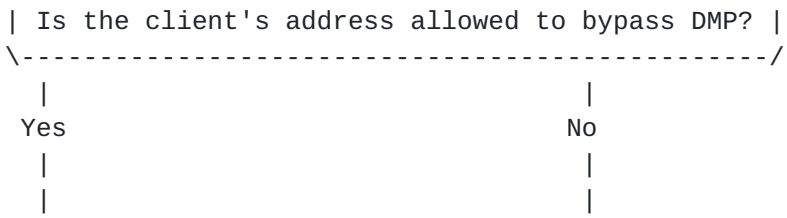
A server using DMP MAY bypass DMP lookups entirely, for reasons defined by the server's operators. Examples include the client connecting from a network address in an "allow relay" list, a client authenticating using another protocol such as SMTP AUTH, and other reasons. This allows client-only hosts and Mail User Agents (MUAs) to use these servers without requiring their own DMP records.

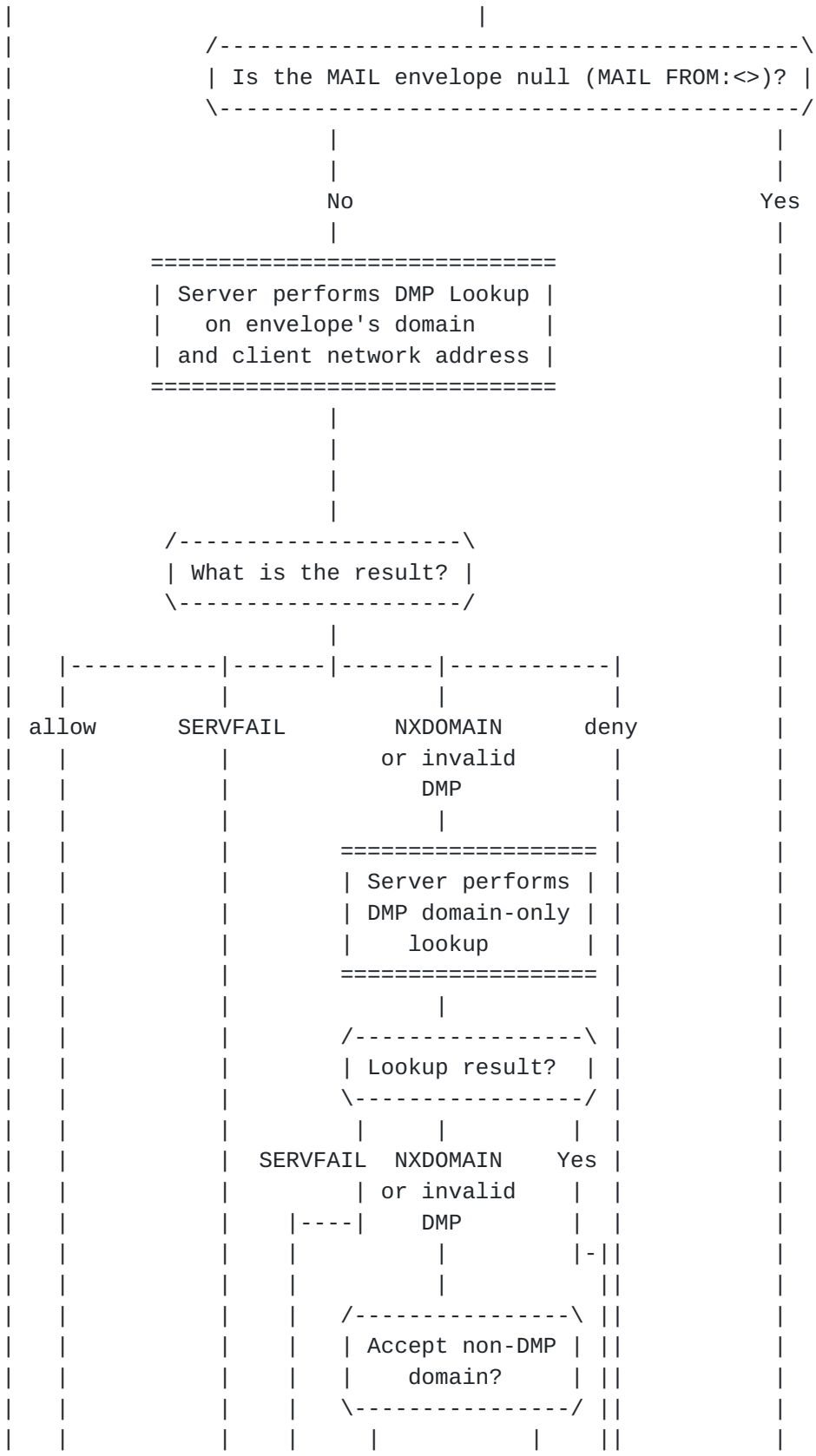
Once a server has DMP query results, the server may act on the message envelope in many ways. The following flowchart demonstrates the RECOMMENDED paths. The chart starts when the client issues the HELO or EHLO command, and ends when the server responds to the MAIL FROM command. Responses allowed to MAIL FROM are from RFC 2821 section 4.3.2.

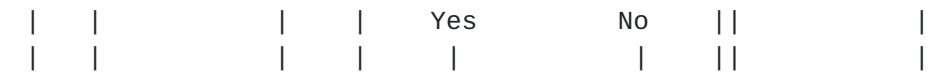
. 250 indicating either HELO/EHLO or MAIL FROM were acceptable
. 451 indicating a local processing error (such as SERVFAIL)
. 550 indicating a rejection based on policy (in this case, the DMP query results and the server's settings determine the policy)

5.1 RECOMMENDED Flowchart




| Is the client's address allowed to bypass DMP? |
\---/
Yes
No


Is the MAIL envelope null (MAIL FROM:<>)?
No
Yes
Server performs DMP Lookup on envelope's domain and client network address
What is the result?
allow
SERVFAIL
NXDOMAIN or invalid DMP
deny
Server performs DMP domain-only lookup
Lookup result?
SERVFAIL
NXDOMAIN or invalid DMP
Yes
Accept non-DMP domain?


Yes
No


(Go to)
(allow)
Allow HELO as alternative?
No
Yes
Server performs DMP on HELO/EHLO FQDN and client address
Lookup result?
allow
deny
(go to)
(allow)
SERVFAIL
(go to)
(fail)
(go to)
(deny)
NXDOMAIN or invalid DMP
Server performs DMP HELO-only FQDN lookup

These examples use IPv4 addresses. The process is identical for other address types.

5.2 Participating Domain's User and Client

```
S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO sender.example.com
S: 250 mail.example.net Hello sender.example.com [192.0.2.1]
C: MAIL FROM:<user@example.com>
```

```
(server looks up 1.2.0.192.in-addr._smtp-client.example.com and
receives "dmp=allow")
S: 250 OK client at 192.0.2.1 verified as authorized sender for
example.com
[resume normally]
```

5.3 Participating Domain, Forwarding Service on Participating Host and Client

```
S: 220 mail.example.net MMS SMTPRCV service v0.9.5
C: HELO othersender.example.org
S: 250 mail.example.net Hello othersender.example.org [192.0.2.5]
C: MAIL FROM:<user@example.com>
(server looks up 5.2.0.192.in-addr._smtp-client.example.com and
receives "dmp=deny")
(server looks up
5.2.0.192.in-addr._smtp-client.othersender.example.org
and receives "dmp=allow")
S: 250 OK client at 192.0.2.5 verified as othersender.example.org
[resume normally]
```

NOTE: The sending domain returned "dmp=deny". To accept this mail, the sending client MUST have a "dmp=allow" record for its HELO host name.

5.4 Null Reverse Path, Participating Host and Client

```
S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO sender.example.com
S: 250 mail.example.net Hello sender.example.com [192.0.2.1]
C: MAIL FROM:<>
(server looks up
1.2.0.192.in-addr._smtp-client.sender.example.com
and receives "dmp=allow")
S: 250 OK client at 192.0.2.1 verified as sender.example.com
[resume normally]
```

5.5 Null Reverse path, Participating Host, Non-Participating Client (dmp=deny)

```
S: 220 mail.example.net MMS SMTPRCV service v0.95
```

```
C: HELO sender.example.com
S: 250 mail.example.net Hello sender.example.com [192.0.2.7]
C: MAIL FROM:<>
(server looks up
7.2.0.192.in-addr._smtp-client.sender.example.com
and receives "dmp=deny")
S: 550 ERROR client at 192.0.2.7 not permitted to send for
sender.example.com
```

[resume as though MAIL FROM has not occurred]

5.6 Null Reverse Path, Participating Host, Non-Participating Client (NXDOMAIN)

S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO sender.example.com
S: 250 mail.example.net Hello sender.example.com [192.0.2.7]
C: MAIL FROM:<>
(server looks up
7.2.0.192.in-addr._smtp-client.sender.example.com
and returns NXDOMAIN)
(server looks up _smtp-client.sender.example.com and receives
"dmp=")
S: 550 ERROR client at 192.0.2.7 not permitted to send for
sender.example.com
[resume as though MAIL FROM had not occurred]

5.7 Non-Participating Domain's User, Non-Participating Client where Server permits Non-Participating Domains

S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO sender.example.com
S: 250 mail.example.net Hello sender.example.com [192.0.2.1]
C: MAIL FROM:<user@example.com>
(server looks up 1.2.0.192.in-addr._smtp-client.example.com
and returns NXDOMAIN)
(server looks up _smtp-client.example.com and returns NXDOMAIN)
S: 250 OK client at 192.0.2.1 not verified as authorized sender for
example.com
[resume normally]

NOTE: The "not verified" response in this example is purely
informational. The server still accepts this e-mail.

5.8 Null Reverse Path, Non-Participating Client where Server permits Non-Participating Domains

S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO sender.example.com
S: 250 mail.example.net Hello sender.example.com [192.0.2.1]

```
C: MAIL FROM:<>
(server looks up
1.2.0.192.in-addr._smtp-client.sender.example.com
and returns NXDOMAIN)
(server looks up_smtp-client.sender.example.com
and returns NXDOMAIN)
S: 250 OK client not verified as sender.example.com
[resume normally]
```

NOTE: The "not verified" response in this example is purely informational.

5.9 Participating Domain's User and Client where DMP lookup fails (SERVFAIL)

S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO sender.example.com
S: 250 mail.example.net Hello sender.example.com [192.0.2.1]
C: MAIL FROM:<user@example.com>
(server looks up 1.2.0.192.in-addr._smtp-client.example.com and returns with SERVFAIL)
S: 451 ERROR Cannot verify 192.0.2.1 as sender for example.com at this time
[resume as though MAIL FROM had not occurred]

NOTE: A participating server SHOULD attempt the lookup more than once before returning a 451 response.

5.10 Participating Domain's User, Non-Participating Client where client host DMP lookup fails (dmp=deny, SERVFAIL)

S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO othersender.example.org
S: 250 mail.example.net Hello othersender.example.org [192.0.2.7]
C: MAIL FROM:<user@example.com>
(server looks up 7.2.0.192.in-addr._smtp-client.example.com and receives "dmp=deny")
(server looks up 7.2.0.192.in-addr._smtp-client.othersender.example.org and returns SERVFAIL)
S: 451 ERROR Cannot verify 192.0.2.7 as sender for othersender.example.org at this time
[resume as though MAIL FROM had not occurred]

NOTE: The sending domain returned "dmp=deny". For this mail to be accepted, the sending client MUST have a "dmp=allow" record for its host name. See example 5.3. In the above case, the server MUST respond with a temporary error and not a permanent one.

5.11 Participating Domain's User, Not Participating Domain's Client

(dmp=deny, NXDOMAIN)

```
S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO othersender.example.org
S: 250 mail.example.net Hello othersender.example.org [192.0.2.7]
C: MAIL FROM:<user@example.com>
(server looks up 7.2.0.192.in-addr._smtp-client.example.com
and receives "dmp=deny")
```

(server looks up
7.2.0.192.in-addr._smtp-client.othersender.example.org
and returns NXDOMAIN)
S: 550 ERROR client at 192.0.2.7 may not send for example.com
[resume as though MAIL FROM had not occurred]

NOTE: In this example, the sending domain returned "dmp=deny". For this mail to be accepted, the sending client MUST have a "dmp=allow" record for its host name. See example 5.3. By comparison, if NXDOMAIN or "dmp=deny" is received, the sending domain's records take precedence.

5.12 Participating Domain's User, Non-Participating Domain's Client (NXDOMAIN plus "dmp=", NXDOMAIN)

S: 220 mail.example.net MMS SMTPRCV service v0.95
C: HELO othersender.example.org
S: 250 mail.example.net Hello othersender.example.org [192.0.2.7]
C: MAIL FROM:<user@example.com>
(server looks up 7.2.0.192.in-addr._smtp-client.example.com
and returns NXDOMAIN)
(server looks up _smtp-client.example.com and receives "dmp=")
(server looks up
7.2.0.192.in-addr._smtp-client.othersender.example.org and returns
NXDOMAIN)
S: 550 ERROR client at 192.0.2.7 may not send for example.com
[resume as though MAIL FROM had not occurred]

NOTE: In this example, the sending domain did not return a record for the client address but does publish DMP records. For this mail to be accepted, the sending client MUST have a "dmp=allow" record for its host name. See example 5.3. By comparison, if NXDOMAIN or "dmp=deny" is received, the sending domain's records take precidence.

6. Other Actions Permitted

Servers querying DMP records MAY take other actions in addition to, or instead of, the actions recommended in Section 5.

Such other actions include adding extra headers to e-mail that identify the DMP query results, so recipients may filter it with their client software. Server administrators MAY switch the order of lookups around, or omit some lookups, to suit their purposes.

Domains and hosts with published DMP records provide receiving servers with the means to identify the publisher's permitted SMTP

clients. What receiving servers' administrators do with this information is left to them.

7. SMTP Source Routing

While depreciated by RFC 2821, some Mail Transfer Agents support SMTP Source Routing, where the sender can define a path through which hosts the e-mail passes through.

An example sender envelope, used in the MAIL command, may look like this:

MAIL FROM:<@mta1.example.com,@mta2.example.com:user@example.com>

If the receiving server supports source routing, it MAY perform its DMP lookups on the first domain or host specified, as this is where the client should be. In the above example, that would be mta1.example.com. Otherwise, the receiving server MUST perform its lookup on the last domain, in this case example.com.

This is equivalent to the receiver querying only the HELO or EHLO host name of the client.

8. Network Overhead and Effectiveness

In November 2003, volunteers provided MTA logs allowing a realistic measurement of DMP's impact. [LOGS]

The test simulated published DMP records by using a test domain labeled "dmptest.invalid" published on a DNS server. The test domain did not contain wildcard records.

The DMP lookup application measured the total size of the DNS query and response packets, minus the amount used to identify ".dmptest.invalid", and added the SMTP message size to this total upon an "allow" condition. The test used the combination of options that permitted the most mail: Allow mail from non-DMP domains and

allow HELO/EHLO records to override a "deny" record from a domain.

From these logs, and a sampling of 19791 domains over a period of eighteen months, came the following measurements. These measurements DID NOT take DNS caching (Time-to-live, or TTL) into account.

DMP's network usage alone, compared to the bandwidth used by SMTP:

. DMP caused an average additional 4.15% increase in bandwidth.

. 12635 (63%) of domains sampled caused a 4.15% or less increase.
. 6281 (33%) of domains sampled caused a 1% or less increase.

DMP's network usage plus the reduction in SMTP bandwidth by refusing "spoofed" messages, compared to the bandwidth used by SMTP alone:

. Frequently "spoofed" domains with correct DMP records used 10% to 20% LESS bandwidth, including the bandwidth used by DMP.
. Less-frequently "spoofed" domains with correct DMP records used 0% to 1% more bandwidth.
. Domains without correct DMP record sets used 1% to 4.15% or more bandwidth.

DNS server caching, with reasonably high TTL values for DMP records, will reduce the network overhead caused by DMP dramatically. Even without considering TTL, popular domains with correct DMP record sets saved up to 20% in SMTP bandwidth, while costing those domains only 1% additional bandwidth, or less.

9. Security Considerations

9.1 DNS Security

DMP depends solely on DNS to publish DMP records. Any compromise of records of a domain would make that domain vulnerable to "spoofing." Likewise, a compromised DNS server hosting an upper-level domain could publish false records for multiple domains.

Best current practices for DNS server security will prevent these and similar abuses and DMP records may reside on DNSSEC servers without changes to DMP.

9.2 Mail Transfer Agent Security

A compromised host authorized through DMP records of a domain may send unauthorized mail in the name of the domain. Likewise, a compromised host with a DMP record set for its Fully Qualified Domain Name may send unauthorized mail in its name. This is critical in that a compromised host with DMP records may send mail

in the name of any domain.

Best current practices for SMTP Mail Transfer Agents in general will prevent these and similar abuses. DMP may permit administrators to identify hosts with compromised MTAs rapidly.

9.3 "Global Wildcard" DMP Records

A domain publishing DMP records may try designating another network, not controlled by them, or the entire Internet as permitted to send mail on its behalf, such as:

```
$ORIGIN example.com.
*._smtp-client TXT "dmp=allow"
```

This not only defeats the purpose of DMP, but administrators of servers using DMP may refuse mail in the name of this domain, regardless of origin, upon discovery of such a record.

In any case, only the network protocol portion of the DMP records may include this type of record, for example:

```
$ORIGIN example.com.
_smtp-client TXT "dmp="
*._smtp-client TXT "dmp=deny"
*.in-addr._smtp-client TXT "dmp=allow"
```

This obtains the desired result without creating invalid DMP records.

Appendix A. Answers to Common Questions and Concerns

The two most common concerns appear here. Others will appear in a DMP Frequently Asked Questions document.

A.1 Does DMP cause some mailing lists and clients that forward e-mail to be refused?

Not anymore, provided the receiving servers will permit a client's HELO or EHLO identifier as an alternative source for DMP records. The policies of the receiving domain will dictate this.

Using a host's records in this manner shifts responsibility from the administrators of the domain to the administrators of the host.

A.2 How does DMP affect SMTP clients on dynamically configured hosts?

Because DMP queries use the client's network address as well as its host or domain name, a change in a client's address could result in returns of NXDOMAIN or "dmp=deny".

Servers using DMP may bypass DMP for "allowed" clients, and such servers may act as relays or smart hosts for such clients. The administrators of the sender domain MUST designate this relay as allowed to send mail for their domain. This is the RECOMMENDED way

to send mail from a dynamically configured host to a domain querying DMP records.

However, administrators MAY dynamically change DMP records alongside of Address records or Mail Exchange records, permitting a dynamically configured host to send mail directly to recipient servers that query DMP records. Note that DNS propagation delays and high Time-to-live (TTL) values may affect the ability to designate a dynamically configured host as a sender.

Appendix B: Proposed Extensions to DMP

To ease the administration of DMP records, many readers provided suggestions to extend DMP. These are the most common suggestions.

B.1 Designating Another Domain's Mailers

A network that sends mail for multiple domains may find a full set of DMP records for each domain inconvenient.

To reduce the administrative burden, a domain may declare the published DMP records of another domain as authoritative for this domain.

This domain only needs one DMP record to accomplish this:

_smtp-client.$DOMAIN. TXT "dmp=altdomain:$ALTDOMAIN."

$DOMAIN is the original domain. $ALTDOMAIN is the fully qualified domain whose designated mailers may also send mail on behalf of $DOMAIN. For consistency with other DNS record names, the $ALTDOMAIN MUST have a trailing period to identify this as a fully qualified domain.

A domain may specify multiple domains, whose senders may be used, with each fully qualified domain separated by commas:

_smtp-client.$DOMAIN. TXT "dmp=altdomain:$ALTDOMAIN1.,$ALTDOMAIN2."

The limit to this would be the limit to the size of a TXT RR record.

One drawback to this extension is the increase in DNS traffic. A server querying DMP records would need to repeat the queries for each of the designated domains. The flowchart in 5.1 would repeat the domain query for each $ALTDOMAIN specified, before querying the host itself if configured to do so, or until "dmp=allow" was found.

Example default DMP record:

```
$ORIGIN example.com.
_smtp-client TXT "dmp=altdomain:example.net.,example.org."
```

B.2 Identifying the Role of Domain, Host or Forwarder

A default DMP record may identify the role of the domain, be it host only or multi-host domain, be it permitted to forward mail in the name of another domain or not.

Following the example in B.1, keywords could include "domain", "forwarder", "host", "altdomain", and so on.

. domain: This is an e-mail domain whose sender envelopes are <$USER@$DOMAIN>, with one or more addresses permitted to send mail on behalf of the domain and its users. A domain may also be a host.
. host: This is a single host, whose permitted sender envelopes include <$USER@$HOST> and Null <>. A domain designating this host's network address as a sender may also permit envelopes for its domain from this host.
. forwarder: This is a single host that may send mail on behalf of other domains. Any envelope may originate from this host, and it implies the functionality of "host".
. altdomain: This domain designates another domain's DMP records as authoritative for this domain. This keyword would override any other keywords in the returned DMP record.

These keywords would appear in the domain or host's default DMP record. A resulting lookup could return "dmp=domain,host,forwarder". "altdomain" would override any other keyword.

This has the potential to solve certain kinds of forgeries, by identifying what a host or domain intends to have the domain or host do. For instance, a host that does not forward mail could not send mail on behalf of other domains. This would allow servers querying DMP to refuse mail from a compromised host, while still permitting Null Sender envelopes and mail sent in the name of the host.

The default of "dmp=" would assume "dmp=domain". A domain with a

misspelled keyword or a keyword with incorrect parameters would appear as a non-participating domain with invalid DMP records.

References

Normative References

[RFC 2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

[RFC 2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001

[RFC 1034] Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", RFC 1034, November 1987

Informative References

[RFC 1464] Rosenbaum, R., "Using the Domain Name System To Store Arbitrary String Attributes", RFC 1464, May 1993

[LOGS] The logs used to obtain this information are available from the Pan-Am Internet DMP web site, at <http://www.pan-am.ca/dmp/dmp-logs.zip>, in Microsoft Access 97 and plain text formats. The archive is approximately 18 MB in size.

Contributors

Raymond S Brand, Lawrence Sherzer and Richard W Rognlie developed the Designated Relays Inquiry Protocol (DRIP), a work-in-progress. DMP uses portions of DRIP to support some mail forwarding systems.

Hadmut Danisch originally approached the idea of publishing a list of hosts to permit mail for a domain; a work-in-progress called the Reverse Mail Exchanger (RMX) DNS Resource Record.

Derek J. Balling <dredd@megacity.org> provided the initial design of

the DMP DNS record template. "der Mouse"
<mouse@rodents.montreal.qc.ca> generalized it, resulting in the
current form.

Michael A. Smith provided a format for the actual contents of DMP
records, based on RFC 1464.

Jack Bates assisted with supporting SMTP Source Routing.

Steve Atkins and Bill Cole assisted with their DNS expertise.

"der Mouse" assisted with testing and with formatting IPv6 versions of DMP records.

NOTE to RFC Editor: "der Mouse" does not wish to be identified by his real name.

Members of the IMS Users mailing list contributed MTA logs and ran a statistics gathering application to obtain the information in Chapter 8. Piotr Kubala provided the majority of this information.

Author's Addresses

Gordon Fecyk
24 - 482 Young Street
Winnipeg, MB R3B 2S6
Canada
Email: gordonf@pan-am.ca

Full Copyright Statement