

# EMAILCORE WG

## Interim meeting, December 2021

Chairs:

Alexey Melnikov <[alexey.melnikov@isode.com](mailto:alexey.melnikov@isode.com)>

Todd Herr <[todd.herr@valimail.com](mailto:todd.herr@valimail.com)>

# Note Well

- This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.
- As a reminder:
  - By participating in the IETF, you agree to follow IETF processes and policies.
  - If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
  - As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
  - Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
  - As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (<https://www.ietf.org/contact/ombudsteam/>) if you have questions or concerns about this.

# Note Well

## (continued)

- Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:
  - BCP 9 (Internet Standards Process)
  - BCP 25 (Working Group processes)
  - BCP 25 (Anti-Harassment Procedures)
  - BCP 54 (Code of Conduct)
  - BCP 78 (Copyright)
  - BCP 79 (Patents, Participation)
  - <https://www.ietf.org/privacy-policy/> (Privacy Policy)

# IETF Code Of Conduct Guidelines RFC 7154

- Treat colleagues with respect
- Speak slowly and limit the use of slang
- Dispute ideas by using reasoned argument
- Use best engineering judgment
- Find the best solution for the whole Internet
- Contribute to the ongoing work of the group and the IETF

# Administrivia

- This Zoom session is being recorded
- Zoom:
  - <https://us06web.zoom.us/j/89359071984?pwd=ZXZSOVBtc0RPWUI1RjhUUGIRZzZQQQT09>
- Jabber room (discussions/back channel):
  - [emailcore@jabber.ietf.org](mailto:emailcore@jabber.ietf.org)
- Shared note taking:
  - <https://notes.ietf.org/notes-emailcore-interim-dec-2021>
- **Note taker?**

# Agenda

- Agenda bashing, administrivia, note well (chairs) - 5 mins
- #17 (Deprecated Source Routes) <<https://trac.ietf.org/trac/emailcore/ticket/17>>
- #9 (G.7.3. Definition of domain name in Section 2.3.5) <<https://trac.ietf.org/trac/emailcore/ticket/9>>
- #15 (G.7.9. Discussion of 'blind' copies and RCPT) <<https://trac.ietf.org/trac/emailcore/ticket/15>>
- #55 (G.14. The FOR Clause in Received header field: Semantics, Security Considerations, and Other Issues) <<https://trac.ietf.org/trac/emailcore/ticket/55>>
- #4 (Exploders seem to be prohibited from adding List-\* header fields) <<https://trac.ietf.org/trac/emailcore/ticket/4>>
- #12 (G.7.5. Improve description/definition of mailing lists, aliases, and forwarding) <<https://trac.ietf.org/trac/emailcore/ticket/12>>
- #3 (G.3. Meaning of "MTA" and Related Terminolog) <<https://trac.ietf.org/trac/emailcore/ticket/3>>

# RFC 5321

G.7.10. Further clarifications needed to deprecated source routes?

<https://trac.ietf.org/trac/emailcore/ticket/17>

Background: RFC 5321 says that source routes are deprecated since 1989, yet at the same time servers must accept them and there are various SHOULDs about whether they can be ignored or rejected by servers, and about when clients can generate them. It also talks about using source routing to work around temporary DNS problems and for mail system debugging.

Agreement on how to deal with this: **strip the document of all mentioning of handling of source routes in text and ABNF, other than to specify their historical use in RFC 821 and point to RFC 821 for implementations that want to implement them for backward compatibility.**

Few minor remaining issues on the following slides.

# RFC 5321

G.7.10. Further clarifications needed to deprecated source routes?

## 4.1.1.3. RECIPIENT (RCPT)

2nd paragraph in -07:

The forward-path consists of the required destination mailbox. When mail reaches its ultimate destination, ***the SMTP server inserts it into the destination mailbox*** in accordance with its host mail conventions.

John commented: above is new text, per notes from Alexey and Ned, replacing the two paragraphs and text about source routes that used to appear here. However, I'm a little concerned about "ultimate destination" as used here. The earlier text was about source routes and that term was defined as "the forward-path contains only a destination mailbox)". But, without that context and discussions about MDAs and what they might do, I am not sure I know what the term means or if it is appropriate to talk about SMTP servers inserting things in mailboxes if we can avoid it.



# RFC 5321

## G.7.10. Further clarifications needed to deprecated source routes?

### 4.1.1.3. RECIPIENT (RCPT)

```
// (JcK 20211202) The examples below appear to have been carried
// forward from RFC821, i.e., before RFC 974 and MX records. Nothing
// in them is actually wrong given the current (as of version -07 of
// this draft), but it seems to me that we should trim it
// aggressively, add a few comments explaining why a proper DNS setup
// with MX records would be a better solution for some of these
// cases, and/or move the examples to Appendix F.2.
```

This command appends its forward-path argument to the forward-path buffer; it does not change the reverse-path buffer nor the mail data buffer.

For example, mail received at relay host [xyz.com](#) with envelope commands

```
MAIL FROM:<userx@y.foo.org>
RCPT TO:<@hosta.int,@jkl.org:userc@d.bar.org>
```

will normally be sent directly on to host [d.bar.org](#) with envelope commands

```
MAIL FROM:<userx@y.foo.org>
RCPT TO:<userc@d.bar.org>
```

# RFC 5321

## G.7.10. Further clarifications needed to deprecated source routes?

### 4.1.1.3. RECIPIENT (RCPT) - continues

As provided in Appendix F.2, [xyz.com](#) MAY also choose to relay the message to [hosta.int](#), using the envelope commands

```
MAIL FROM: <userx@y.foo.org>
```

```
RCPT TO: <@hosta.int,@jkl.org:userc@d.bar.org>
```

or to [jkl.org](#), using the envelope commands

```
MAIL FROM: <userx@y.foo.org>
```

```
RCPT TO: <@jkl.org:userc@d.bar.org>
```

# RFC 5321

G.7.10. Further clarifications needed to deprecated source routes?

## F.2. Source Routing

RFC 821 utilized the concept of explicit source routing to get mail from one host to another via a series of relays. The requirement to utilize source routes in regular mail traffic was eliminated by the introduction of the domain name system "MX" record and the last significant justification for them was eliminated by the introduction, in RFC 1123, of a clear requirement that addresses following an "@" must all be fully-qualified domain names.

***Consequently, the only remaining justifications for the use of source routes are support for very old SMTP clients or MUAs and in mail system debugging. They can, however, still be useful in the latter circumstance and for routing mail around serious, but temporary, problems such as problems with the relevant DNS records.***

-This section likely needs rewriting. If yes, how?-

# RFC 5321

G.7.10. Further clarifications needed to deprecated source routes?

## F.2. Source Routing (continued)

SMTP servers **MUST** continue to accept source route syntax as specified in the main body of this document and in RFC 1123. They **MAY**, if necessary, ignore the routes and utilize only the target domain in the address. If they do utilize the source route, the message **MUST** be sent to the first domain shown in the address. In particular, a server **MUST NOT** guess at shortcuts within the source route.

Clients **SHOULD NOT** utilize explicit source routing **except under unusual circumstances, such as debugging or potentially relaying around firewall or mail system configuration errors.**

-This section likely needs rewriting. If yes, how?-

# RFC 5321

## G.7.3. Definition of domain name in Section 2.3.5

<https://trac.ietf.org/trac/emailcore/ticket/9>

### 2.3.5. Domain Names

Paragraph 2 and 3:

The domain name, as described in this document and in RFC 1035 [4], is the entire, fully-qualified name (often referred to as an "FQDN"). A domain name that is not in FQDN form is no more than a local alias. ***Local aliases MUST NOT appear in any SMTP transaction.***

Only resolvable, fully-qualified domain names (FQDNs) are permitted when domain names are used in SMTP. In particular, names that can be resolved to MX RRs or address (i.e., A or AAAA) RRs (as discussed in Section 5) are permitted, as are CNAME RRs whose targets can be resolved, in turn, to MX or address RRs. ***Local nicknames or unqualified names MUST NOT be used. There are two exceptions to the rule requiring FQDNs:***

- \* The domain name given in the EHLO command MUST be either a primary host name (a domain name that resolves to an address RR) or, if the host has no name, an address literal, as described in Section 4.1.3 and discussed further in the EHLO discussion of Section 4.1.4.
- \* The reserved mailbox name "postmaster" may be used in a RCPT command without domain qualification (see Section 4.1.1.3) and MUST be accepted if so used.

# RFC 5321

## G.7.3. Definition of domain name in Section 2.3.5

<https://trac.ietf.org/trac/emailcore/ticket/9>

### 2.3.5. Domain Names

Paragraph 3:

Only **resolvable**, fully-qualified domain names (FQDNs) are permitted when domain names are used in SMTP. ***In particular, names that can be resolved to MX RRs or address (i.e., A or AAAA) RRs (as discussed in Section 5) are permitted, as are CNAME RRs whose targets can be resolved, in turn, to MX or address RRs.*** Local nicknames or unqualified names MUST NOT be used.

Problem: "resolvable" can be interpreted that a receiving server needs to attempt to resolve them when received, as opposed to resolving them when they need to be used (e.g. relaying to the next hop/for delivery).

**Suggestion:** remove "resolvable" above. Point to section 5 about resolving FQDNs, as it already talks about A/AAAA:

Only fully-qualified domain names (FQDNs) are permitted when domain names are used in SMTP. Local nicknames or unqualified names MUST NOT be used. [...continue with the text about 2 exceptions...]

See section 5 for details definition of how FQDNs are resolved.

# RFC 5321

## G.7.9. Discussion of 'blind' copies and RCPT

<https://trac.ietf.org/trac/emailcore/ticket/15>

In Section 7.2. "Blind" Copies

Addresses that do not appear in the message header section may appear in the RCPT commands to an SMTP server for a number of reasons. The two most common involve the use of a mailing address as a "list exploder" (a single address that resolves into multiple addresses) and the appearance of "blind copies".

OLD (remainder of this paragraph):

***Especially when more than one***

RCPT command is present, and in order to avoid defeating some of the purpose of these mechanisms, SMTP clients and servers ***SHOULD NOT*** copy ***the full set*** of RCPT command arguments into the header section, either as part of trace header fields or as informational or private-extension header fields.

# RFC 5321

## G.7.9. Discussion of 'blind' copies and RCPT

<https://trac.ietf.org/trac/emailcore/ticket/15>

OLD (remainder of this paragraph):

***Especially*** when more than one RCPT command is present, and in order to avoid defeating some of the purpose of these mechanisms, SMTP clients and servers **SHOULD NOT** copy ***the full set*** of RCPT command arguments into the header section, either as part of trace header fields or as informational or private-extension header fields.

NEW (***Proposal 1***):

When more than one RCPT command is present, and in order to avoid defeating some of the purpose of these mechanisms, SMTP clients and servers **MUST NOT** copy **any** of RCPT command arguments into the header section, either as part of trace header fields or as informational or private-extension header fields.

NEW (***Proposal 2***):

In order to avoid address disclosures that are problematic, in terms of privacy, any copying of a RCPT command argument into the message header section **MUST** be restricted to only the one used for delivery to the recipient getting the specific version of the message that discloses that address.



# RFC 5321

## G.14. The FOR Clause in Received header field: Semantics, Security Considerations, and Other Issues

<https://trac.ietf.org/trac/emailcore/ticket/55>

### 4.4.1. Received Header Field

4th paragraph:

- \* If the FOR clause appears, it MUST contain exactly one <path> entry, even when multiple RCPT commands have been given. Multiple <path>s raise some security issues and have been deprecated, see Section 7.2.

Proposal to add:

- \* If the FOR clause appears, it MUST contain exactly one <path> entry, even when multiple RCPT commands have been given, **and that <path> entry MUST contain one of the addresses that caused the message to be routed to the recipient of this message copy.** Multiple <path>s raise some security issues and have been deprecated, see Section **7.2**.

Should this point to Section 7.2 ("Blind" Copies), Section 7.6 (Information Disclosure in Trace Fields), or even both?

# RFC 5321

## G.14. The FOR Clause in Received header field: Semantics, Security Considerations, and Other Issues

<https://trac.ietf.org/trac/emailcore/ticket/55>

### 7.6. Information Disclosure in Trace Fields

In some circumstances, such as when mail originates from within a LAN whose hosts are not directly on the public Internet, trace (e.g., "Received") header fields produced in conformance with this specification may disclose host names and similar information that would not normally be available. This ordinarily does not pose a problem, but sites with special concerns about name disclosure should be aware of it. ***Also, the optional FOR clause should be supplied with caution or not at all when multiple recipients are involved lest it inadvertently disclose the identities of "blind copy" recipients to others.***

Remove the last sentence or fix it?

Any special considerations for MSAs?

# RFC 5321

Exploders seem to be prohibited from adding List-\* header fields

<https://trac.ietf.org/trac/emailcore/ticket/4>

## 3.9. Aliases and Mailing Lists

An SMTP-capable host SHOULD support both the alias and the list models of address expansion for multiple delivery. When a message is delivered or forwarded to each address of an expanded list form, the return address in the envelope ("MAIL FROM:") MUST be changed to be the address of a person or other entity who administers the list.

However, in this case, ***the message header section*** (RFC 5322 [12]) ***MUST be left unchanged***; in particular, the "From" field of the header section is unaffected.

Problem: "MUST be left unchanged" seems to prohibit addition of header fields. Also some mailing lists add tags to Subject header fields. And DMARC workaround strategies result in modified From.

Proposal (replace the last 2 sentences with):

When a message is delivered or forwarded to each address of an expanded list form, the return address in the envelope ("MAIL FROM:") MUST be changed to be the address of a person or other entity who administers the list. This change to MAIL FROM doesn't affect the header section of the message.

# RFC 5321

G.7.5. Improve description/definition of mailing lists, aliases, and forwarding

<https://trac.ietf.org/trac/emailcore/ticket/12>

The next few slides display current text about mailing lists and aliases. When discussing them, please consider the following question: **is the current definition broken or is it good enough?**

- clarifications and/or adding extra examples is fine
- the bar for changing the definition completely is high and need to have strong WG consensus

# RFC 5321

G.7.5. Improve description/definition of mailing lists, aliases, and forwarding

<https://trac.ietf.org/trac/emailcore/ticket/12>

## 3.9. Aliases and Mailing Lists

2nd paragraph:

An important mail facility is a mechanism for multi-destination delivery of a single message, by transforming (or "expanding" or "exploding") a pseudo-mailbox address into a list of destination mailbox addresses. When a message is sent to such a pseudo-mailbox (sometimes called an "exploder"), copies are forwarded or redistributed to each mailbox in the expanded list. Servers **SHOULD** simply utilize the addresses on the list; application of heuristics or other matching rules to eliminate some addresses, such as that of the originator, is strongly discouraged. We classify such a pseudo-mailbox as an "alias" or a "list", depending upon the expansion rules.

# RFC 5321

G.7.5. Improve description/definition of mailing lists, aliases, and forwarding

<https://trac.ietf.org/trac/emailcore/ticket/12>

## 3.9.1. Simple Aliases

To expand an alias, the recipient mailer simply replaces the pseudo-mailbox address in the envelope with each of the expanded addresses in turn; the rest of the envelope and the message body are left unchanged. The message is then delivered or forwarded to each expanded address.

Note forwarding as an email address portability issue? If we do, is this something for A/S? Or just an example here?

Suggestion to add an example explaining how this works.

Suggestion to do no further changes.

# RFC 5321

## G.3. Meaning of "MTA" and Related Terminology

<https://trac.ietf.org/trac/emailcore/ticket/3>

G.3. Meaning of "MTA" and Related Terminology

A terminology issue has come up about what the term "**MTA**" actually refers to, a question that became at least slightly more complicated when we formalized RFC 6409 Submission Servers. Does the document need to be adjusted to be more clear about this topic? Note that the answer may interact with the question asked in Section 2 above.

Possibly along the same lines, RFC 2821 changed the RFC 821 terminology from "**sender-SMTP**" and "**receiver-SMTP**" to "**SMTP client**" and "**SMTP server**" respectively. As things have evolved, it is possible that newer terminology is a source of confusion and that the terminology should be changed back, something that also needs discussion.

Question 1: "**sender-SMTP**" and "**receiver-SMTP**" versa "**SMTP client**" and "**SMTP server**". Proposal: no change.

Question 2: definition of MTA (next slide)

# RFC 5321

## G.3. Meaning of "MTA" and Related Terminology

<https://trac.ietf.org/trac/emailcore/ticket/3>

### 2.3.3. Mail Agents and Message Stores

Additional mail system terminology became common after RFC 821 was published and, where convenient, is used in this specification. In particular, SMTP servers and clients provide a mail transport service and therefore act as "**Mail Transfer Agents**" (MTAs). "**Mail User Agents**" (MUAs or UAs) are normally thought of as the sources and targets of mail. At the source, an MUA might collect mail to be transmitted from a user and hand it off to an MTA or, more commonly in recent years, a specialized variation on an MTA called a "**Submission Server**" (MSA) [42]. . At the other end of the process, the final ("delivery") MTA would be thought of as handing the mail off to an MUA (or at least transferring responsibility to it, e.g., by depositing the message in a "message store"). However, while these terms are used with at least the appearance of great precision in other environments, the implied boundaries between MUAs and MTAs often do not accurately match common, and conforming, practices with Internet mail. Hence, the reader should be cautious about inferring the strong relationships and responsibilities that might be implied if these terms were used elsewhere

Proposal: no change, unless the above text is broken.



# Done for today

Don't forget to preserve Zoom chat for posterity!