Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-heejin-domainbasedemailaddressing-00
Published: 17 February 2023
Intended Status: Informational
Expires: 21 August 2023
Authors: HJ. Lee, Ed.
Kakao Corp.

Proposed Specification for Domain-based Email Addressing

Abstract

This document proposes a new email addressing specification that allows email messages to be sent to all email addresses associated with a domain. The new format can simplify the email addressing process and reduce the risk of errors, while maintaining compatibility with existing email protocols and standards. This specification includes requirements, design, and security considerations for the new email addressing format.

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 https://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 21 August 2023.

Copyright Notice

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Sending emails to multiple recipients within the same domain can be a time-consuming and inefficient process, particularly when individual email addresses must be manually entered. The goal of this proposed specification is to simplify the email addressing process by allowing messages to be sent to all email addresses associated with a domain using the domain name, rather than individual email addresses. By enabling email messages to be sent to all email addresses within a domain with just the domain name, this specification will significantly reduce the time and effort required to send emails to multiple recipients. Additionally, this specification will help reduce errors, simplify the email addressing process, and make it easier to send messages to large groups of recipients within the same domain.

2. Motivation

The current email addressing system can be inefficient and time-consuming, especially when sending messages to multiple email addresses within the same domain. This often requires manually entering each email address, which can be prone to errors and can significantly slow down the email sending process. Moreover, as the number of recipients increases, it becomes even more challenging to manage and keep track of all the individual email addresses. The proposed specification aims to simplify the email addressing process by enabling emails to be sent to all email addresses associated with a domain using the domain name, rather than individual email addresses. This will save time and effort for users, as they will no longer have to manually enter each email address. Additionally, this

will make it easier to send messages to large groups of recipients within the same domain, improving communication efficiency in organizations and among groups of individuals. Finally, by reducing errors and streamlining the email addressing process, this specification has the potential to make email communications more reliable and effective.

3. Requirements

The proposed email addressing specification must fulfill the following requirements to achieve the goals of simplifying the email addressing process and reducing errors: 1. All email addresses associated with a domain must be included in the recipient list when the domain name is used as the recipient address. 2. The email must be delivered to all intended recipients within the domain, including those with email addresses that are not explicitly specified. 3. The specification must work within the constraints of existing email protocols and standards, such as the Simple Mail Transfer Protocol (SMTP) and the Domain Name System (DNS). 4. The new addressing format must be backwards-compatible with existing email clients and servers, allowing messages to be sent between systems that have not yet adopted the new specification. 5. The specification must not introduce new security vulnerabilities or increase the risk of spam or other malicious activities. 6. The specification should be designed in such a way as to be easily adopted and integrated into existing email systems, minimizing the cost and complexity of implementation.

4. Design

The proposed email addressing specification will use the existing domain name as the recipient address, rather than individual email addresses. When a message is sent using this new format, the email server will retrieve a list of all email addresses associated with the domain name from the Domain Name System (DNS) records. The email server will then deliver the message to all email addresses associated with the domain name, including those that are not explicitly specified in the recipient list. This will ensure that all intended recipients within the domain receive the message, even if their email address was not specifically included in the recipient list. To ensure backwards compatibility with existing email clients and servers, messages sent using the new addressing format will include both the domain name and the individual email addresses of all recipients in the header of the email. This will enable email clients and servers that have not yet adopted the new specification to continue to process messages in the existing format. To minimize the risk of spam and other malicious activities, the email addressing specification will include measures to verify the authenticity of the sender and the domain name. For example,

email servers may use the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to verify the domain name and prevent spam and spoofing. Overall, the new email addressing format will simplify the email addressing process, reduce errors, and improve communication efficiency, while also maintaining compatibility with existing email protocols and standards.

5. Security Considerations

The proposed email addressing specification introduces a new way to address email messages and must take into account potential security risks associated with this new approach. The following security considerations must be taken into account when implementing the specification: 1. Sender Authentication: To prevent email spoofing, it is essential to verify the authenticity of the sender. The Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) can be used to authenticate the domain name and ensure that the email has not been altered in transit. 2. Email Privacy: The specification must ensure that email content is kept private and not accessible to unauthorized third parties. Transport Layer Security (TLS) can be used to encrypt email messages in transit, preventing unauthorized interception and disclosure of email content. 3. Domain Reputation: The new addressing format could be used by spammers to send unsolicited emails, which can harm the reputation of the domain. Implementing DKIM and DMARC (Domain-based Message Authentication, Reporting and Conformance) protocols can help mitigate this risk by ensuring that only authorized senders can use the domain to send emails. 4. Denial of Service (DoS) Attacks: The specification must be designed to prevent DoS attacks, which can be used to overwhelm email servers and disrupt email services. To mitigate this risk, email servers can implement rate-limiting or throttling to limit the number of messages that can be sent in a given time period. 5. Implementation Risks: The specification should be implemented with care to avoid introducing new vulnerabilities or compromising the security of existing email systems. Implementers should thoroughly test the specification and consider the potential impact of any changes before deploying it in a production environment. By taking into account these security considerations, the new email addressing specification can provide a secure and reliable way to send emails using domain names, while also reducing the risk of spam, spoofing, and other security threats.

6. Scenario

Acme Corporation is a company that has recently adopted the proposed email addressing specification. Prior to the adoption of this new format, employees at Acme had to manually enter the email addresses of their intended recipients, which was often time-consuming and prone to errors. However, with the new email addressing format,

employees can simply enter the domain name of their intended recipients, and the email will be sent to all email addresses associated with that domain. For example, if an employee at Acme wants to send an email to all employees at their subsidiary company, "Acme Subsidiary," they can simply enter "@acmesubsidiary.com" into the To: field of their email client. The email will be sent to all email addresses associated with that domain, including those of employees who work in different departments, locations, or roles. This saves time and reduces the risk of errors that can occur when manually entering email addresses. Furthermore, the new email addressing format can simplify the process of managing email addresses for the IT department at Acme. Instead of having to manage individual email addresses for each employee, they can simply manage the email addresses associated with each domain. This reduces the complexity and potential errors associated with managing individual email addresses for a large organization. Overall, the adoption of the proposed email addressing specification has streamlined the email communication process at Acme Corporation, saving time and reducing errors while maintaining compatibility with existing email protocols and standards.

7. Conclusion

The proposed email addressing specification provides a simple and efficient way to address email messages using domain names. By enabling email messages to be sent to all email addresses associated with a domain, this new format can simplify the email addressing process and reduce the risk of errors. At the same time, the specification maintains compatibility with existing email protocols and standards, enabling messages to be exchanged between systems that have not yet adopted the new format. The security considerations have been taken into account, and the new format includes measures to prevent email spoofing, protect email privacy, and prevent DoS attacks, among other security risks. Overall, the proposed email addressing specification is a practical and useful solution that can benefit both email senders and recipients. By facilitating efficient communication and reducing the risk of errors and security threats, this new format can enhance the reliability and usefulness of email as a communication tool.

8. IANA Considerations

This memo includes no request to IANA.

9. Security Considerations

This document does not affect Internet security.

10. References

10.1. Normative References

10.2. Informative References

[RFC5321] Klensin, J., RFC 5321., "Simple Mail Transfer Protocol", 2008.

[RFC5322] Resnick, P., RFC 5322., "Internet Message Format", 2008.

[RFC6530] Klensin, J., RFC 6530., "Overview and Framework for Internationalized Email", 2012.

[RFC6854] Resnick, P., RFC 6854., "Update to Internet Message Format to Allow Group Syntax in the "From:" and "Sender:" Header Fields", 2013.

Author's Address

Heejin Lee (editor)
Kakao Corp.

Email: dependency@kakao.com