ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 3, pp: (24-27), Month: July – September 2026, Available at: www.researchpublish.com

The World Runs on Port 25

Qasim T. Zaidi[1]

Saudi Arabian Oil Company, Dhahran, Kingdom of Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.21368061

Published Date: 14-July-2026

Abstract: **This article explores SMTP's historical development, architecture, and the critical role Port 25 plays in both public and private infrastructures. It also covers the simplicity and further gets into complexity, while being the most relied upon protocol on the planet. SMTP Port 25 remains the standard for server-to-server communication across the internet.**

Keywords: **SMTP, Port 25, Email Security, Microsoft Exchange, Mail Flow, Open Relay, Receive Connectors.**

I. INTRODUCTION

Simple Mail Transfer Protocol (SMTP), the cornerstone of global email communication, continues to operate largely on Port 25/TCP despite newer secure alternatives. This paper explores SMTP's historical development, architecture, and the critical role Port 25 plays in both public and private infrastructures. The technical structure of SMTP, email transmission flow, and the difference between secure and insecure channels are examined. We also investigate how internal SMTP relays enable non-authenticating devices such as scanners and printers to function within corporate infrastructures, and how Microsoft Exchange receive connectors are configured to support both internal and external email flows. The paper concludes by examining how the world continues to rely on SMTP and Port 25, supported by global email traffic statistics and trends over the past two decades.

II. HISTORY

The Simple Mail Transfer Protocol (SMTP) is the original and still-dominant protocol that facilitates email transmission across networks. It was formally introduced in August 1982 by Dr. Jon Postel of the University of Southern California's Information Sciences Institute, through the publication of Request for Comments 821 (RFC 821). SMTP was designed during a time when the internet itself was in its infancy, and email was rapidly becoming a critical tool for academic and governmental communication.

SMTP operates as a text-based, connection-oriented protocol layered over TCP/IP. It uses Port 25 as its default channel for transmitting emails between servers (Mail Transfer Agents). While newer submission ports such as 587 (for client submission) and 465 (for SSL) have been introduced, Port 25 remains the standard for server-to-server communication across the internet.

The protocol's simplicity was part of its original appeal, but that simplicity also introduced challenges over time—such as lack of encryption, authentication, and susceptibility to spam and spoofing. As email usage expanded globally in the 1990s and 2000s, SMTP evolved with additional standards including STARTTLS, SPF, DKIM, and DMARC, yet its core transport model over Port 25 remains widely deployed and indispensable.

III. CASE STUDY

In this paper, we examine how SMTP operates today, the ways it has been hardened, and the unique configurations required within enterprise environments to ensure its reliable and secure delivery. SMTP was originally designed without any built-in security. Messages were sent in plain text, leaving them vulnerable to interception, tampering, and spoofing. To address this, secure variants were introduced. RFC 2487 (1999) introduced STARTTLS, an extension allowing SMTP to negotiate encryption using TLS without changing ports. This enables backward compatibility while allowing secure transmission when supported by both client and server.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 3, pp: (24-27), Month: July – September 2026, Available at: www.researchpublish.com

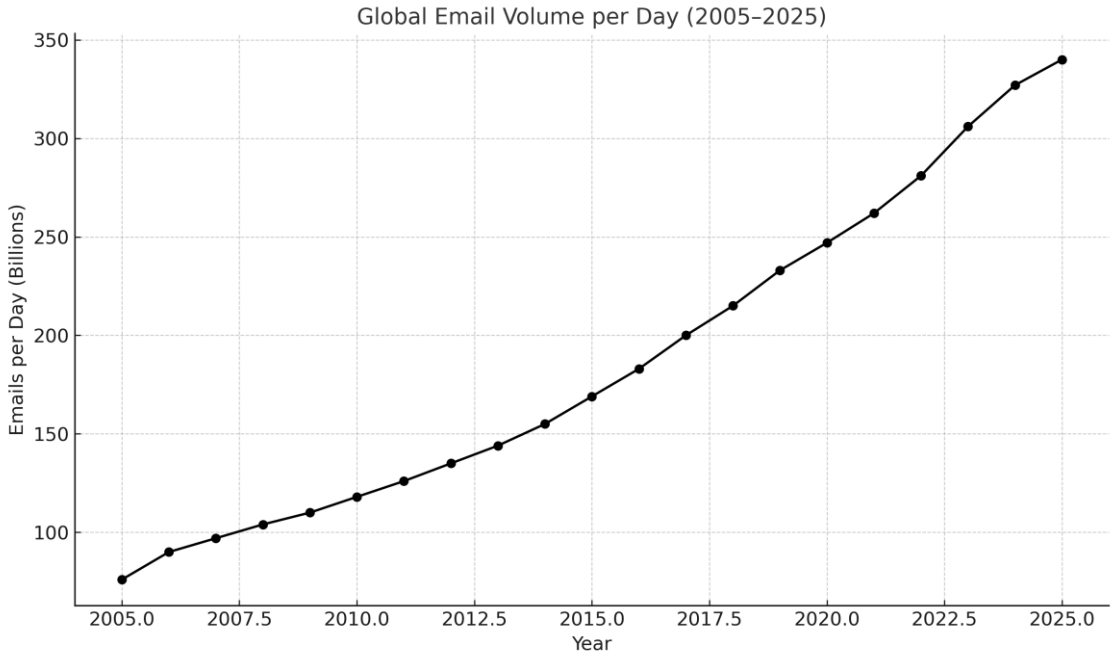

Fig. 1: Global Daily Email Volume (2005–2025)

I. SECURE VS INSECURE SMTP TRANSMISSION

Another alternative is SMTPS, using port 465 for implicit SSL encryption. Though deprecated for a time, it has regained popularity. However, port 25 remains the primary channel for MTA-to-MTA communication, meaning that opportunistic encryption is only as good as the weakest link.

Without proper TLS enforcement policies, messages may fall back to unencrypted transmission. Administrators must ensure TLS is configured and enforced, and use policies like MTA-STS or DANE (RFC 7672) to guarantee message security.

II. EMAIL TRANSMISSION OVER THE PUBLIC INTERNET

When an email is sent from one domain to another, it typically follows this path: client submits message to outbound MTA → DNS MX lookup → recipient MTA → mailbox storage.

Throughout this journey, security and authenticity are key concerns. The following standards protect email integrity:
- RFC 7208 (SPF): Lists authorized sending servers

- RFC 6376 (DKIM): Digitally signs email headers

- RFC 7489 (DMARC): Aligns SPF/DKIM with policy and reporting

Without these, spam and phishing campaigns can impersonate domains with ease. While widely adopted, these tools require accurate DNS and cooperative adoption across ecosystems.

III. INTERNAL OPEN RELAYS IN CORPORATE ENVIRONMENTS

Printers, scanners, and legacy systems in enterprises often cannot authenticate with SMTP. Instead, organizations set up internal relays to accept unauthenticated messages from trusted internal IP addresses. These devices may relay through an Exchange server, IIS SMTP service, or a Linux-based mail server like Postfix.

Best practices include:

- IP whitelisting only
- Domain restrictions (e.g., relay only to @company.com)
- Logging and alerting

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 14, Issue 3, pp: (24-27), Month: July – September 2026, Available at: www.researchpublish.com

Improperly configured relays risk becoming 'open relays'—allowing abuse for spam campaigns. RFC 5321 (SMTP) explicitly warns against such scenarios.

Fig. 2: Internal SMTP Relay Flow for Printers and Applications

IV. SMTP GATEWAYS AND MICROSOFT EXCHANGE RECEIVE CONNECTORS

Inbound email from the internet is first received by an SMTP gateway. These may be cloud-based services (e.g., Microsoft Defender, Mimecast) or on-prem appliances (e.g., Cisco IronPort, FortiMail).

These gateways provide filtering and policy enforcement before handing off clean email to internal servers like Microsoft Exchange.

Exchange uses Receive Connectors (configured via EAC or PowerShell) to accept SMTP messages. Key connector types include:

- Default Frontend: Accepts external unauthenticated email
- Client Frontend: Authenticated submission from clients
- Relay Connectors: Accept email from trusted apps (printers, scanners)

RFC 4409 defines submission standards, while Exchange-specific controls allow tight security management at the transport layer.

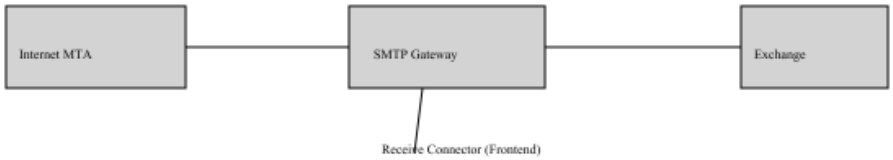

Fig. 3: Exchange Receive Connector Flow from Internet to Mailbox

V. GLOBAL EMAIL TRAFFIC AND DEPENDENCY ON PORT 25

Global email traffic has steadily increased over the last two decades. According to Radicati Group and Statista, daily email volume rose from around 76 billion/day in 2005 to over 340 billion/day in 2025.

Port 25 continues to serve as the backbone for MTA-to-MTA communication despite client migration to ports 587 and 465. Reasons Port 25 persists:

- Default in legacy infrastructure
- Supported by major email providers
- Compatible with DNS-based delivery via MX records

The following table and graph illustrate the growth of email volumes globally:

Table 1: Estimated Global Email Volume per Day (2005–2025)

Year	Emails per Day (Billions)
2005	76
2006	90
2007	97
2008	104
2009	110
2010	118
2011	126
2012	135
2013	144
2014	155
2015	169
2016	183
2017	200
2018	215
2019	233
2020	247
2021	262
2022	281
2023	306
2024	327
2025	340

IV. CONCLUSION

Port 25/TCP remains indispensable in the modern internet. SMTP, while over four decades old, is deeply embedded in every sector—from personal email accounts to cloud services and enterprise infrastructure. Despite challenges like spam, phishing, and unencrypted transmission, continuous evolution through RFCs, security overlays, and policy frameworks have kept it relevant.

Organizations must continue adopting secure configurations (e.g., STARTTLS, SPF, DKIM, DMARC, MTA-STS) while maintaining compatibility with systems dependent on unauthenticated internal relay. Port 25's ubiquity makes it a pillar of email communication—essential, yet invisible, to most internet users.

REFERENCES

[1] Postel, J. 'Simple Mail Transfer Protocol', RFC 821, Aug. 1982.

[2] Klensin, J. 'Simple Mail Transfer Protocol', RFC 5321, Oct. 2008.

[3] Resnick, P. 'Internet Message Format', RFC 5322, Oct. 2008.

[4] Hoffman, P. 'SMTP Service Extension for Secure SMTP over TLS', RFC 2487, Jan. 1999.

[5] Gellens, R. and Klensin, J. 'Message Submission for Mail', RFC 4409, Apr. 2006.

[6] Crocker, D. 'DomainKeys Identified Mail (DKIM)', RFC 6376, Sept. 2011.

[7] Kitterman, S. 'Sender Policy Framework (SPF)', RFC 7208, Apr. 2014.

[8] Hansen, T., et al. 'Domain-based Message Authentication, Reporting, and Conformance (DMARC)', RFC 7489, Mar. 2015.

[9] Statista, Global email statistics (2005–2025), www.statista.com.

[10] Microsoft Docs, 'Understanding Receive Connectors in Exchange'.