Internet Engineering Task Force	H. Lord
Internet-Draft	M. O'Reirdan
Intended status: Informational	J. Rosenwald
Expires: March 15, 2012	Comcast
	September 12, 2011

Recommendations for the transition of email services from IPv4 to IPv6 for Internet Service Providers
draft-oreirdan-rosenwald-ipv6mail-transition-01

Abstract

This document contains a phased plan for how providers of email services can effect and manage the transition of email services from IPv4 to IPv6. It is expected that this will be effected over a period of years and it is unlikely that any transition will completely exclude the ongoing possibility of using IPv4 as a transport mechanism for email. This provides one possible implementation plan for transitioning email services on the Internet from a predominantly IPv4-based connectivity model that suports IPv6.

Status of this Memo

Copyright Notice

Table of Contents

*1. Key Terminology

*2. Introduction and Problem Statement

*3. Important Notice of Limitations and Scope

*4. Transition and a phased model

*5. Phase 1: Preparation Phase

*6. Phase 2: Transition Phase

*7. Phase 3: Post Transition Phase

*8. SMTP Issues raised by transition to IPv6

*9. Webmail issues raised by transition to IPv6

*10. POP3 issues raised by transition to IPv6

*11. IMAP issues raised by transition to IPv6

*12. Abuse Issues

*13. Inbound email issues

*14. Outbound email issues

*15. Security Considerations

*16. Privacy Considerations

*17. IANA Considerations

*18. Acknowledgements

*19. References

*Appendix A. Document Change Log

*Appendix B. Open Issues

*Authors' Addresses

1. Key Terminology

This section defines the key terms used in this document.

1.1. Email

Email is a method of exchanging digital messages from an author to one or more recipients.

1.2. Web mail

A service which offers web based access to email services which would otherwise be accessed by dedicated email programs running on the device used to access the email.

1.3. Host

An end user's host, or computer, as used in the context of this document, is intended to refer to a computing device that connects to the Internet. This encompasses devices used by Internet users such as personal computers, including laptops, desktops, and netbooks, as well as mobile phones, smart phones, home gateway devices, and other end user computing devices which are connected or can connect to the public Internet and/or private IP networks.
Increasingly, other household systems and devices contain embedded hosts which are connected to or can connect to the public Internet and/or private IP networks. However, these devices may not be under interactive control of the Internet user, such as may be the case with various smart home and smart grid devices.

1.4. SMTP

As defined in RFC2821

1.5. POP

As defined in RFC1939 and updated by RFCs 1957, 2449 and 6186

1.6. IMAP

As defined in RFC3501

1.7. Internet Customer

An end user who leverages a connection to the Internet via an ISP and is provisioned with a public IP to communicate on the Internet.

1.8. Internet facing server

A server which is addressed with a public IP address that is able to communicate with other publically addressed servers. A server typically hosts a service that can be utilized by the Internet community.

1.9. Internal users

Known corporate users of the ISP entity.

2. Introduction and Problem Statement

With the depletion of IPv4 address space and the transition of Internet infrastructure to IPv6, it is necessary to address the way in which email services can be transitioned from an IPv4 transport to that of IPv6. It is anticipated that IPv4 will continue for a long time as a major transport mechanism for email services of all sorts. There are significant issues to be addressed around the matter of abuse in an IPv6 based environment which have been addressed and largely resolved when operating using IPv4 as a transport mechanism. The successful resolution of abuse issues may well be a key limitation on the transition of email to an IPv6 environment from the point of view of Internet Service providers.

3. Important Notice of Limitations and Scope

The issues of abuse specific to IPv6 are not yet fully resolved and will need much additional work. The consideration given to abuse issues here should be considered as preliminary and incomplete.

4. Transition and a phased model

It is not reasonable to specify the changes that each and every email system connected to the Internet must undergo in order to achieve the desired transition, as the number of connected systems precludes creating one plan that contains such a level of detail. Further, while there are common scenarios that may be specified for transitioning individual email systems, the specific timeline and mechanisms utilized for a given email system will be unique. Despite these challenges, it is necessary to coordinate expectations on an overall basis so that Internet-wide email services are maintained throughout the transition. This document specifies a three-phase transition plan that includes preparation, transition, and post-transition phases, and delineates the necessary activities within each phase based on the role that an organization plays in the provision and use of email services.
An important distinction made in this transition plan is identifying the explicit requirement for existing end-site organizations to add IPv6-based connectivity to their email servers during a transition phase. An accelerated adoption of IPv6 for email servers enables new organizations in the post-transition phase to be connected to the

Internet only via IPv6 and still have access to the overall set of email servers.

For nearly every organization, the task of IPv6-enabling their email servers is far easier than undertaking an organization-wide adoption of IPv6. Still, the requirement for existing Internet-connected organizations to add IPv6 connectivity (even to a small number of email systems) will be a significant hurdle and require a level of effort that may not be achievable given the lack of compelling additional benefits to these organizations [RFC1669]. This transition plan presumes that "connectivity is its own reward" [RFC1958] and that there still exists a sufficient level of cooperation among Internet participants to make this evolution possible. The adoption of a slow rollout and phased approach will reduce risk and provide additional insight to abuse issues so that further understanding can be gained and solutions developed.

The three proposed phases are: Preparation Phase, Transition Phase, and Post-Transition Phase.

5. Phase 1: Preparation Phase

In the Preparation Phase, Service Providers pilot their IPv6 email services, and end-site organizations prepare to provide email services via IPv6-based connectivity while continuing to provide email services via IPv4 connectivity. During the Preparation Phase, the following principles apply:

PREP1: Service Providers SHOULD offer pilot IPv6-based email service to their Internet customers for outbound email submission to the Service Providers outbound mail servers. IPv6-based email services MAY be provided via IPv6 transition mechanisms (such as those described in [RFC4213], for example) or via native IPv6 network service. This SHOULD be on an infrastructure separate from the IPv4 infrastructure and on a unique service names from that used for production IPv4 traffic.

PREP2: Organizations SHOULD arrange for IPv6-based Internet connectivity for any Internet facing email servers sending, outbound servers (smtp) or receiving email, inbound servers (mx). Internet-facing email servers in this phase SHOULD use separate service names per [RFC4472] to avoid impact to production IPv4-based services unless the organization supports production IPv6 connectivity.

PREP3: Organizations MAY provide IPv6-based email services to internal user communities. This would be connectivity from IPv6 addressed employee computers to the corporate mail servers.

6. Phase 2: Transition Phase

In the Transition Phase, Service Providers offer production IPv6 and IPv4 services to their Internet customers. End-site organizations provide Internet-facing services in a production manner via IPv6- based connectivity in addition to IPv4-based connectivity. During the Transition Phase, the following principles apply:

TRANS1: Service Providers MUST offer IPv6-based email service to their Internet customers. IPv6-based email service SHOULD be via native IPv6 network service but MAY be via IPv6 transition mechanisms if necessary.
TRANS2: Organizations MUST arrange for IPv6-based Internet connectivity for any Internet-facing servers (e.g., web, email, and domain name servers). Internet-facing IPv6 servers SHOULD be treated as production by the organization, and SHOULD be treated as production by other Internet organizations.
TRANS3: Organizations SHOULD provide IPv6-based email service to their internal user communities.

7. Phase 3: Post Transition Phase

In the Post-Transition Phase, end-site organizations MUST provide all email services via IPv6-based connectivity, thus allowing for new Internet customers connected solely by IPv6. During the Post-Transition Phase, the following principles apply:
POST1: Service Providers MUST offer IPv6-based email service to their Internet customers. IPv6-based email service SHOULD be via native IPv6 network service.
POST2: Organizations MUST arrange for IPv6-based Internet connectivity for any Internet-facing email servers. Internet-facing IPv6 email servers MUST be treated as production by the organization, and SHOULD be treated as production by other Internet organizations.
POST3: Organizations SHOULD provide IPv6-based email service to internal user communities and send email via IPv6.
POST4: Service Providers MAY continue to offer IPv4-based email service to their Internet customers. Organizations MAY continue to use IPv4-based email service. However, IPv6 SHOULD be preferred when the option exists to use both services.

8. SMTP Issues raised by transition to IPv6

This section will cover issues around the use of SMTP in an IPv6 based infrastructure.

9. Webmail issues raised by transition to IPv6

This section will cover issues around the use of Webmail in an IPv6 based infrastructure.

10. POP3 issues raised by transition to IPv6

This section will cover issues around the use of POP3 in an IPv6 based infrastructure.

11. IMAP issues raised by transition to IPv6

This section will cover issues around the use of IMAP in an IPv6 based infrastructure.

12. Abuse Issues

The lack of a full understanding of all abuse threats SHOULD NOT preclude the adoption of IPv6 for mail. A comprehensive understanding of threats will not be available until implementation.

13. Inbound email issues

Domain Authentication SHOULD be required and MUST utilize the mechanisms outlined in RFC4871, RFC5585 and RFC5617
Consideration should be given to a "known sender list" for a limited number of email servers which are verified as belonging to authorized sources of email which will be given volume allowance commensurate with their expected behavior and exempt from the restrictive throttles applied to unknown senders. It is likely that these would be the email servers of large ISPs, well known email senders such as major Email service providers and other verified sources
Given the scale of the IPv6 address space, the possibility that a connection exhaustion scenario may develop where the number of attempted connections to an individual email service may overwhelm its ability to provide service. This may occur either deliberately as part of an abusive scenario or inadvertently due to misconfiguration.
Common filtering techniques that are critical for early decision making such as real-time blocklists and IP reputation will need to be amended for practical use in an IPv6 environment. Other reputation keys such as CIDR reputation and domain reputation should be considered.

14. Outbound email issues

Submitting of unauthenticated port 25 mail to outbound IPv6 email servers MUST be prohibited. User authentication MUST be required to allow users to submit email for delivery. Users MUST therefore be required to authenticate on port 587 or 465 for outbound email submission.
In environments where IP reputation is tracked for outbound customers, this is likely to occur for ISPs that do not require authentication for sending email outbound. Single IP reputation will become obsolete.
Consideration will have to be made for tracking reputation per CIDR. CIDR reputation would continue to track reputation at the lowest unit currently maintained which is the customer residence. The ISP will know this allocation for their customers and therefore can rely on this information for reputation tracking.
Public announcement and aggregation of IPv6 addresses into the delegated CIDR blocks will be required for the purpose of identification and tracking of a single entity. CIDR reputation can then be applied to the whole entity. There will need to be a mechanism to infer or accurately lookup the CIDR allocation.
Throttling, particularly when off-net sending is allowed, should be considered.

Utilization of 6to4 conversion (modem to server (6) and server to external server (4)) can be an intermediate step as described above. Utilization of NAT technologies may also obscure the source IP address. Given the scale of the IPv6 address space, the possibility that a connection exhaustion scenario may develop where the number of attempted connections to an individual email service may overwhelm its ability to provide service. This may occur either deliberately as part of an abusive scenario or inadvertently due to misconfiguration.

15. Security Considerations

This document does not address any security issues inherent in IPv6 itself. It acknowledges that there are as yet unresolved abuse issues specific to deploying email infrastructures based on an IPv6 transport. Abuse issues includes spam, phishing and spoofing of email addresses.

16. Privacy Considerations

This document describes at a high level activities that ISPs should be sensitive to, where the collection or communication of PII may be possible. In addition, when performing this transition, ISPs should be careful to protect any PII collected whether deliberately or inadvertently.
As noted, any sharing of data from the user to the ISP and/or authorized third parties should be done on an opt-in basis. Additionally the ISP and or authorized third parties should clearly state what data will be shared and with whom the data will be shared with.
Lastly,there my be legal requirements in particular legal jurisdictions concerning how long any subscriber-related or other data is retained, of which an ISP operating in such a jurisdiction should be aware and with which an ISP should comply.

17. IANA Considerations

There are no IANA considerations in this document.

18. Acknowledgements

The authors wish to acknowledge the following individuals and groups for performing a detailed review of this document and/or providing comments and feedback that helped to improve and evolve this document:
None as yet
Large section of this document are based on RFC5211 "An Internet Transition Plan" authored by John Curran which outlines an overall transition plan for the Internet from IPv4 to IPv6.

19. References

[RFC1669]

	Curran, J., "Market Viability as a IPng Criteria", RFC 1669, August 1994.
[RFC1939]	Myers, J.G. and M.T. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.
[RFC1957]	Nelson, R., "Some Observations on Implementations of the Post Office Protocol (POP3)", RFC 1957, June 1996.
[RFC1958]	Carpenter, B., "Architectural Principles of the Internet", RFC 1958, June 1996.
[RFC2449]	Gellens, R., Newman, C. and L. Lundblade, "POP3 Extension Mechanism", RFC 2449, November 1998.
[RFC2821]	Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.
[RFC4213]	Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.
[RFC5211]	Curran, J., "An Internet Transition Plan", RFC 5211, July 2008.
[RFC6186]	Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, March 2011.

Appendix A. Document Change Log

[RFC Editor: This section is to be removed before publication]
-01 version:

*-01 version published

Appendix B. Open Issues

[RFC Editor: This section is to be removed before publication]
No open issues to date

Authors' Addresses

Heather Lord Lord Comcast Cable Communications One Comcast Center 1701 John F. Kennedy Boulevard Philadelphia, PA 19103 US EMail: heather_lord@cable.comcast.com URI: http://www.comcast.com

Michael O'Reirdan O'Reirdan Comcast Cable Communications One Comcast Center 1701 John F. Kennedy Boulevard Philadelphia, PA 19103 US EMail: michael_oreirdan@cable.comcast.com URI: http://www.comcast.com

Jordan Rosenwald Rosenwald Comcast Cable Communications One Comcast Center 1701 John F. Kennedy Boulevard Philadelphia, PA 19103 US EMail: jordan_rosenwald@cable.comcast.com URI: http://www.comcast.com