Outbound Port 25 blocking for dynamic IP Addresses

IETF 92

Dallas, Texas, USA

Takehito Akagiri, Rakuten, Inc.

Kaoru Maeda, Lepidum Co. Ltd.

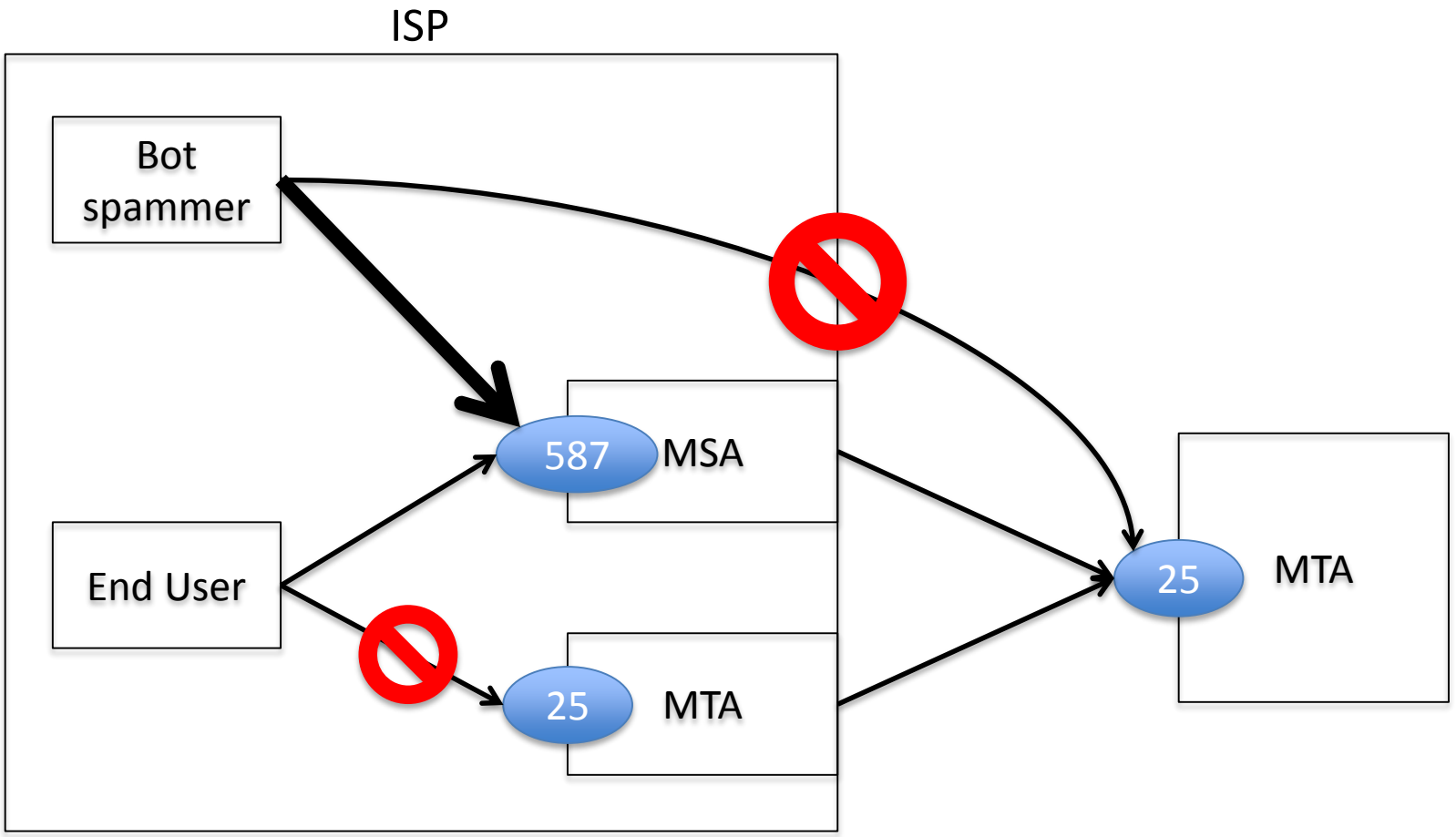
Outline

- What is OP25B?
- Why OP25B?
- How it's done?
- Why now?
- What have done?
- What's next?

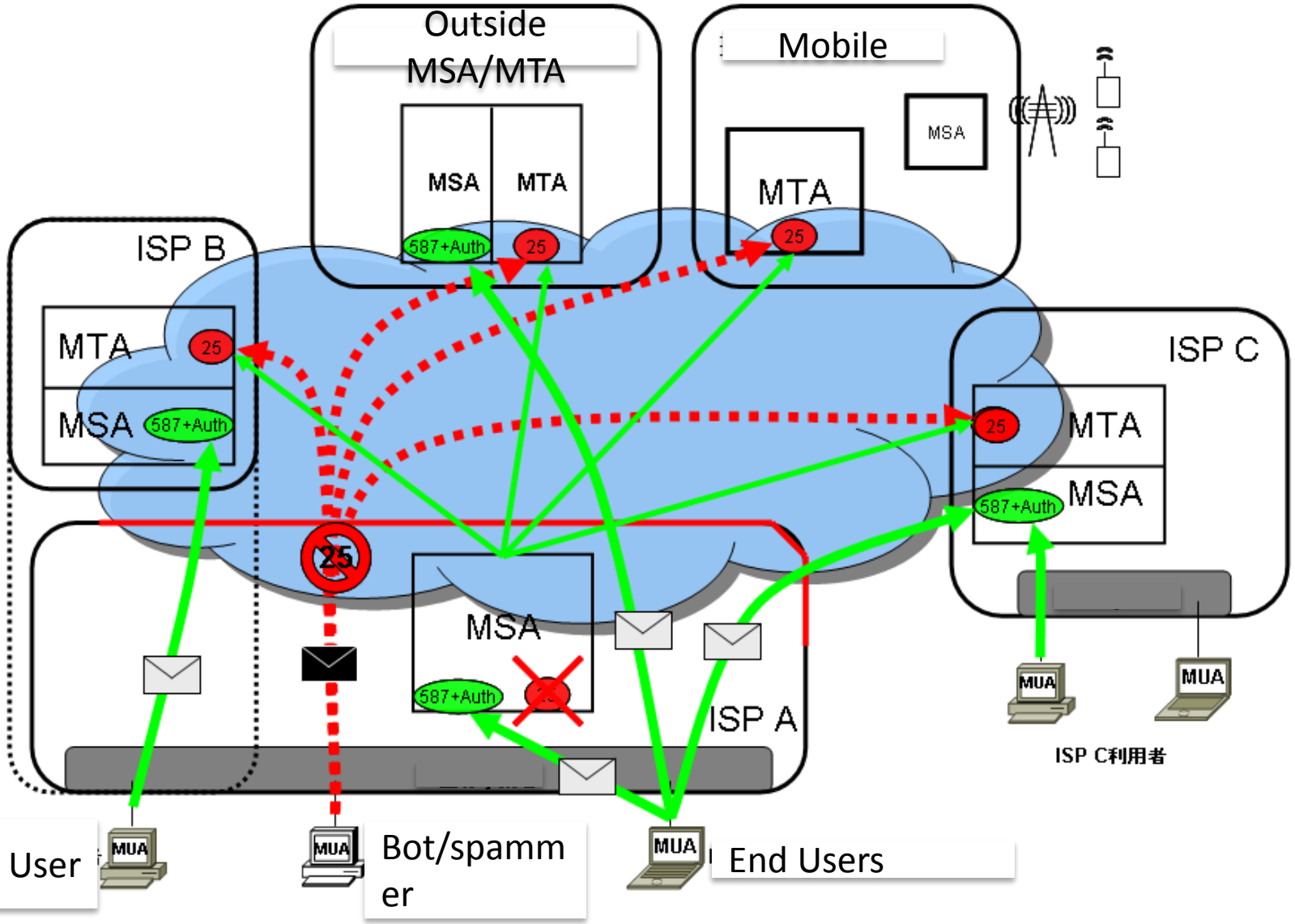
What is OP25B?

- It is about "to block sending email spams"
- OP25B stands for
  "outbound port 25 blocking" for dynamic IP
- Email spam senders under ISP connect to SMTP servers from dynamic IP addresses
  - Block most common traffic path

Quick glance at OP25B



Full-blown OP25B deployment in JP



Why OP25b?

- To stop sending spam at the closest point of the source
  - Not to send, instead of not to receive
  - Less outbound spam traffic
- Countermeasures can focus on:
  - Submission Port + SMTP AUTH
  - Static IP addresses
  - Webmail

Why document now?

- Already adopted widely
  - Japan: De facto standard
  - EU: France Telecom, Telecom Italia, etc.
  - USA: Comcast, AOL, etc.
  - South America: CERT.br
- Documentation wanted
  - Help ISPs that haven't implemented OP25B do it
- Technology got mature enough

How it's done?

- Past practices documented in:
  - http://www.ietf.org/id/draft-akagiri-op25b-dynamicip-00.txt
  - NOTE: This document contains
    - some historical steps needed 10 years ago
    - local situation in Japan
- Should be simpler for ISPs that start now

What have done?

- Past Discussions
  - IRTF – ASRG (2005)
    - http://www.ietf.org/mail-archive/web/asrg/current/msg11920.html
  - MAAWG Recommendation (2005)
  - Widely adopted in Japan around 2005
- Past issues and how solved
  - False blocking of valid submissions
    - Move to submission port 587 with SMTP-AUTH
      - RFC4409, now RFC6409
  - Too many ACLs
    - Router performance improved these years

What's next?

- Update draft to -01
  - Practices for iprv6
  - Remove historical and local parts
- Other communities
  - JANOG works towards BCOP
- In IETF
  - Is appsawg feasible for this draft?