7 Years in the Spam-Wars Trenches. Lessons Learned.

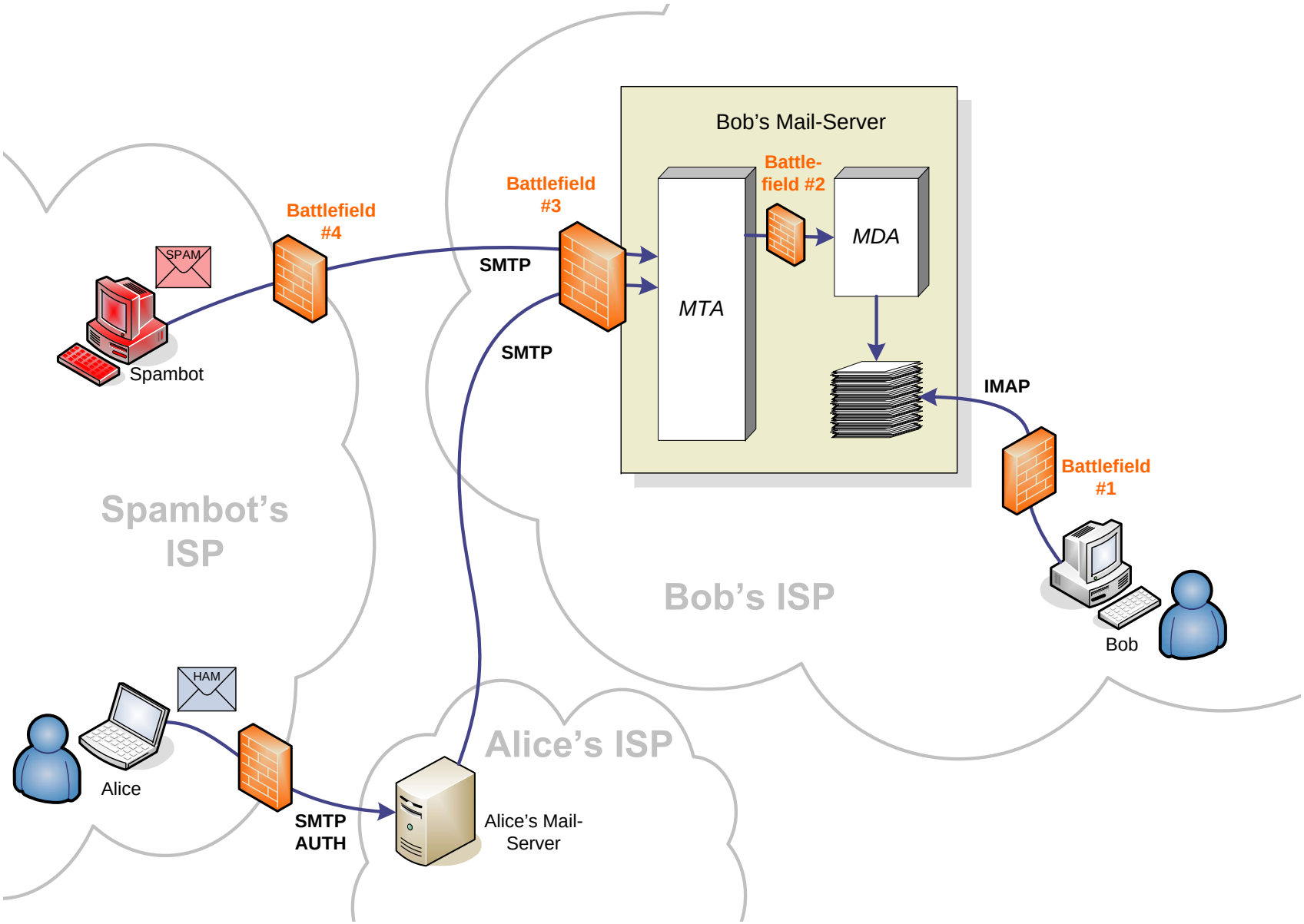
David Schweikert

ISG.EE - ETH Zürich

Linuxforum 2007

About me

- For the last 7 years at the ISG.EE, ETH Zürich
- Main occupations: head of development, postmaster
- Open-source projects:
  Mailgraph, Postgrey, Gedafe, ISGTC
- `http://david.schweikert.ch/`


Bob's Mail-Server
Battlefield #3
Battle-field #2
MDA
MTA
Battlefield #4
SPAM
SMTP
SMTP
Spambot
IMAP
Battlefield #1
Spambot's ISP
Bob's ISP
Bob
HAM
Alice
Alice's ISP
SMTP AUTH
Alice's Mail-Server

MUA: Examples

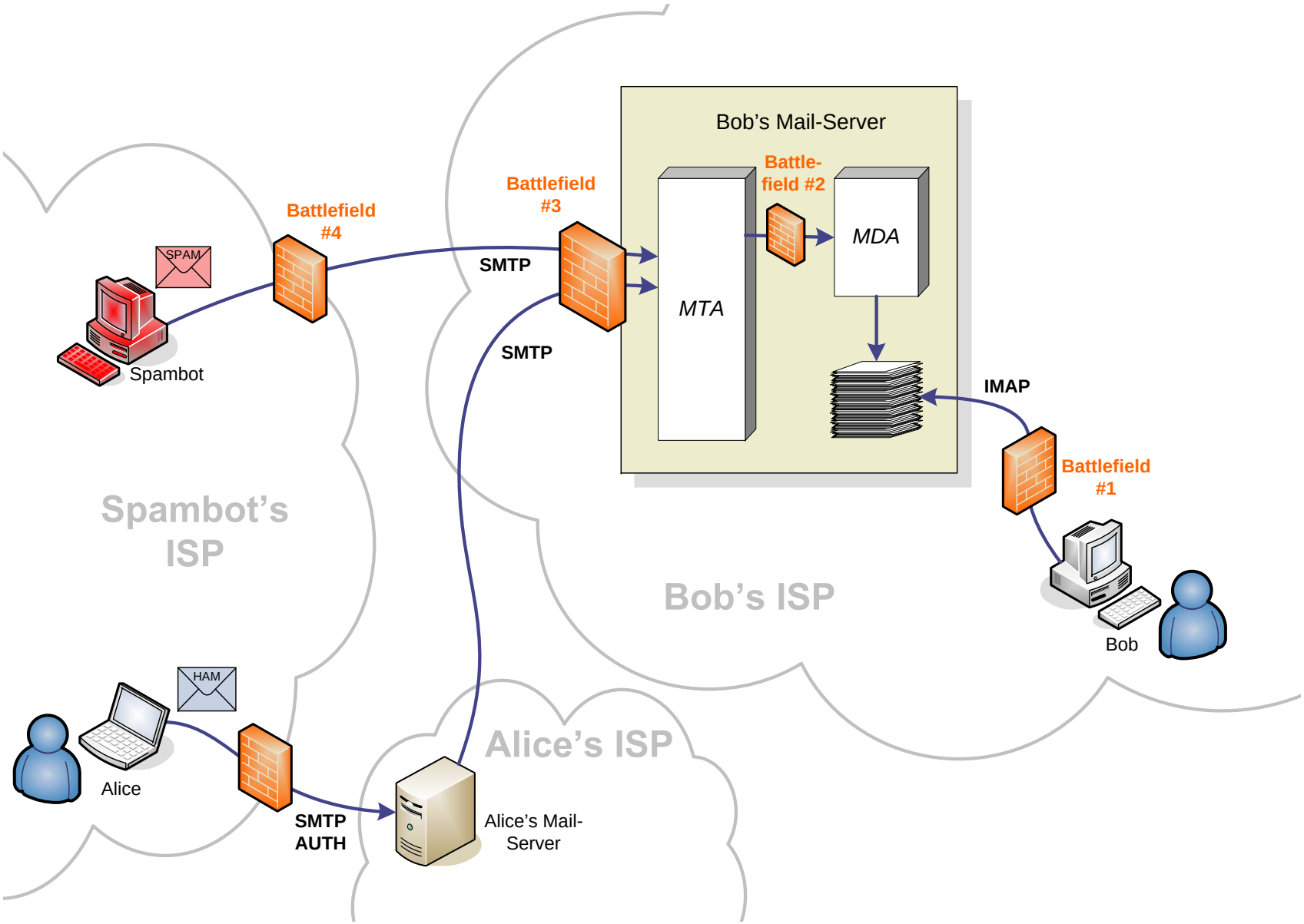
- Thunderbird
- POPFile
- SpamBayes

MUA: Pros

- **You** don't need to do anything
- The **users** are fully in control
- Nice user **interface**

MUA: Cons

- Your **users** need to do it
- Bad on **slow links**
- Lots of mails in the spam folder
  $\rightarrow$ just **delete them all**


Bob's Mail-Server
Battlefield #3
Battle-field #2
MDA
MTA
Battlefield #4
SMTP
SMTP
SPAM
Spambot
IMAP
Battlefield #1
Spambot's ISP
Bob's ISP
Bob
HAM
Alice
Alice's ISP
SMTP AUTH
Alice's Mail-Server

MTA after queue: Examples

Programs:

- Amavisd-new
- SpamAssassin
- DSPAM

Algorithms:

- Heuristics
- Bayes
- Collaborative filters (DCC, Razor)
- RBL/URIBL blacklists
- RFC-checks
- SPF, Sender-ID, DomainKeys

MTA after queue: Pros

- Rather easy to **setup**
- Easy to update **technology**
- Full **flexibility**

MTA after queue: Cons

- If you don't deliver a mail, you told a **lie** to the mail client
- Big **spam folders**
- Difficult **user interaction**

The user should be in control

- It's supposed to be a **service**
- There are always **false positives**
- **Opt-out** is good for low-risk techniques
- **Opt-in** is good for high-risk techniques

Do not throw away detected spam

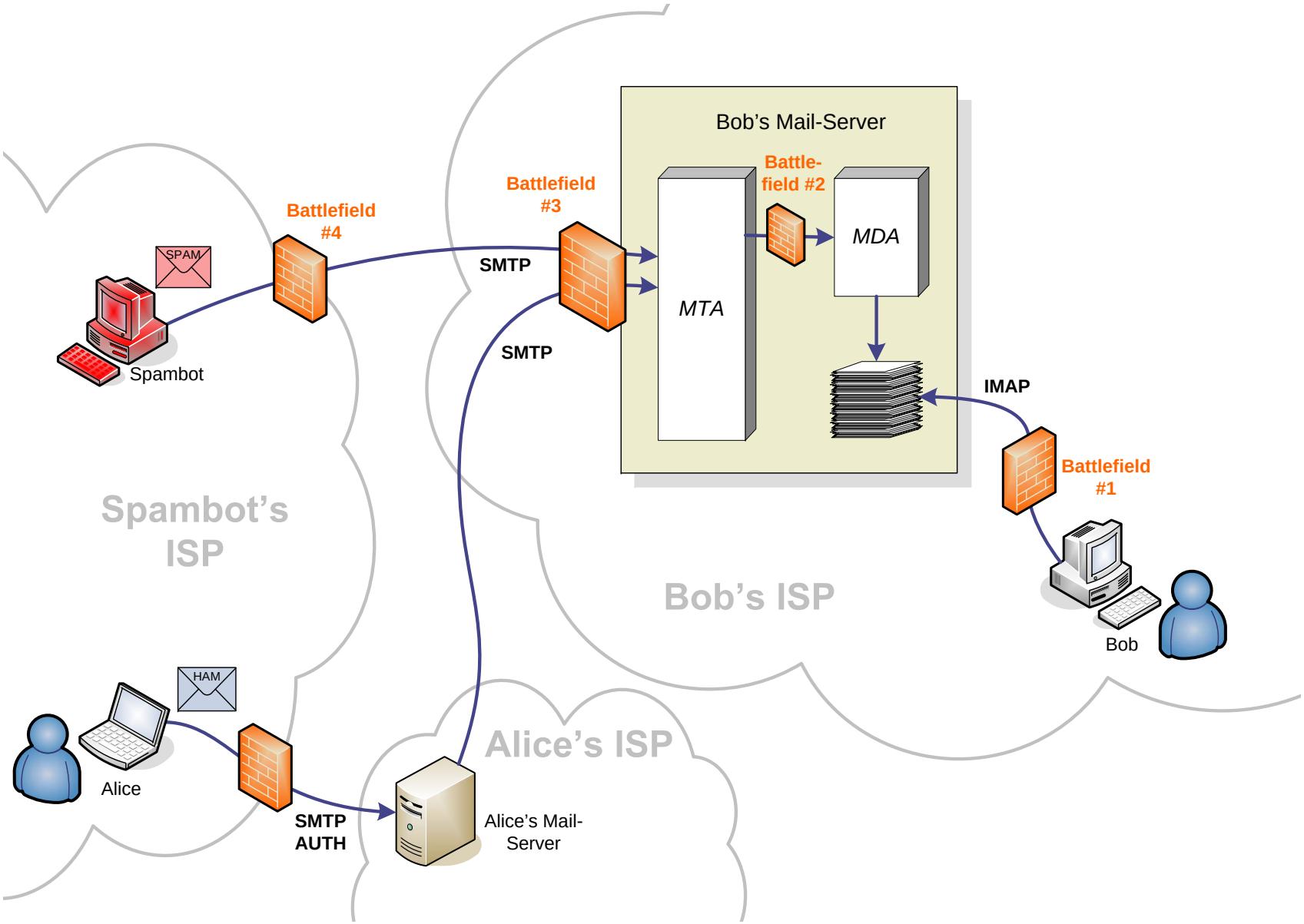
- Do not throw it away, just **mark it**
- Leave the **Subject** line unchanged
- Recommend a **spam folder** instead of /dev/null
- **Exception** to the rule: viruses and phishing mails

Make it the safest as possible

- **Scoring** systems are good (SpamAssassin)
- No **single rule** should be enough
- **Unsafe tests** are OK with a scoring system

Use a global Bayes-DB

- Theory: what is considered spam is **individual**
- Reality: **poorly trained** DBs
- Do per-user Bayes in **Thunderbird**
- Global Bayes: help the **scoring**


Bob's Mail-Server
Battlefield #3
Battle-field #2
MDA
MTA
Battlefield #4
SPAM
SMTP
SMTP
Spambot
IMAP
Battlefield #1
Spambot's ISP
Bob's ISP
Bob
HAM
Alice
Alice's ISP
SMTP AUTH
Alice's Mail-Server

MTA before queue: Pros

- The **sender notices** immediately, that the mail is not going to be delivered
- No **dirty hands**
- Less mails in the **spam-folder**

MTA before queue: Cons

- The mails are **gone**
- The users have little or **no control**
- Tricky **timing** issues

MTA before queue: What to check?

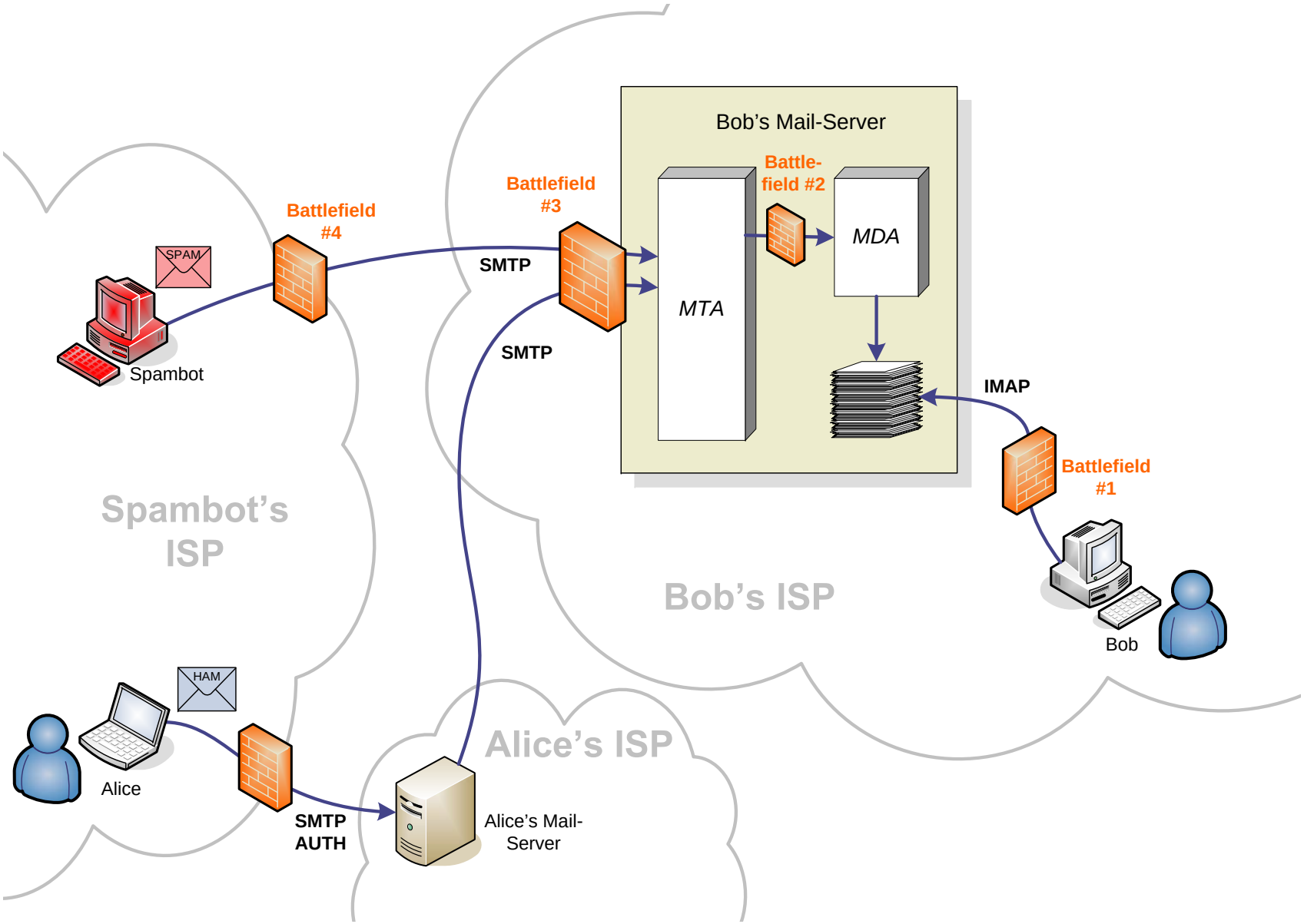
Do NOT use:

- **RBL** blacklists
- **RFC**-checks
- **SPF**, **Sender-ID**, **DomainKeys**
- **Content-Filter**

MTA before queue: What to check?

OK:

- **Sanity** of sender+recip. **addresses**
- **Greylisting**
- **Teergrubing** (Tarpitting)


Bob's Mail-Server
Battlefield #3
Battle-field #2
MDA
MTA
Battlefield #4
SPAM
SMTP
SMTP
Spambot
IMAP
Battlefield #1
Spambot's ISP
Bob's ISP
Bob
HAM
Alice
Alice's ISP
SMTP AUTH
Alice's Mail-Server

Spam-Source: Sender Authentication

- SPF / SenderID
- DomainKeys / DKIM

Consequence:

- Old: send mails through your **local ISP**'s SMTP server
- New: send mails through your **home ISP**'s SMTP server
- SMTP-AUTH

Spam-Source: Port 25 Filtering

More and more providers do:

- **Block** outgoing **port 25** from dialup machines
- Example: WLAN network at the ETH Zurich
- Example: “Swiss ISPs Against Spam” initiative

Spam-Source: Port 25 Filtering

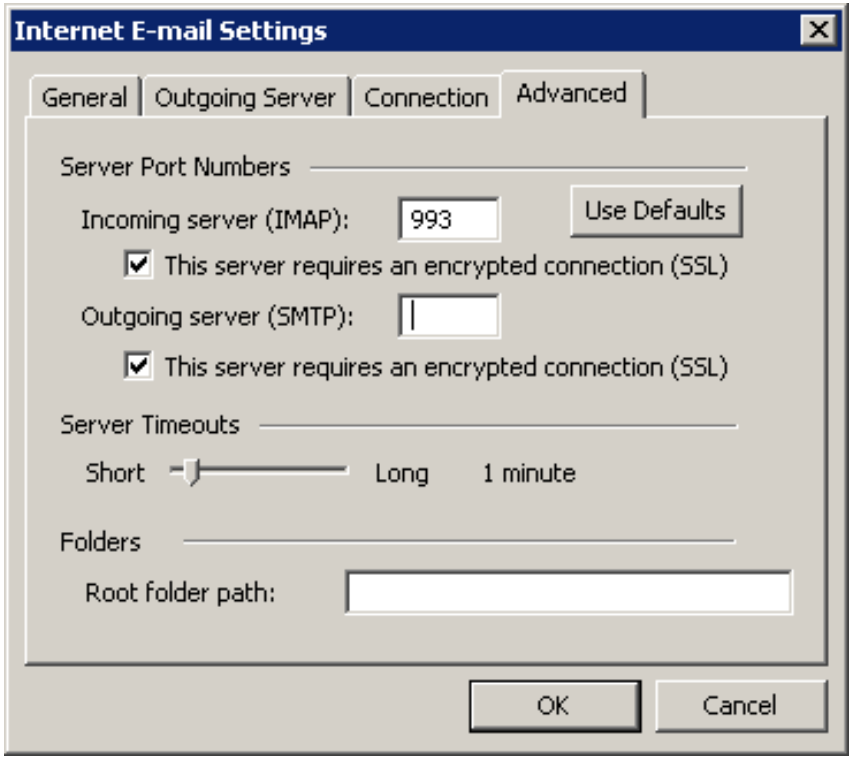
- Breaks SMTP-AUTH!

Solution:

- Implement **port 587** (submission)
- Enforce TLS and SMTP-AUTH

Spam-Source: Port 25 Filtering

Outlook's cleverness:



Where's **TLS** ?

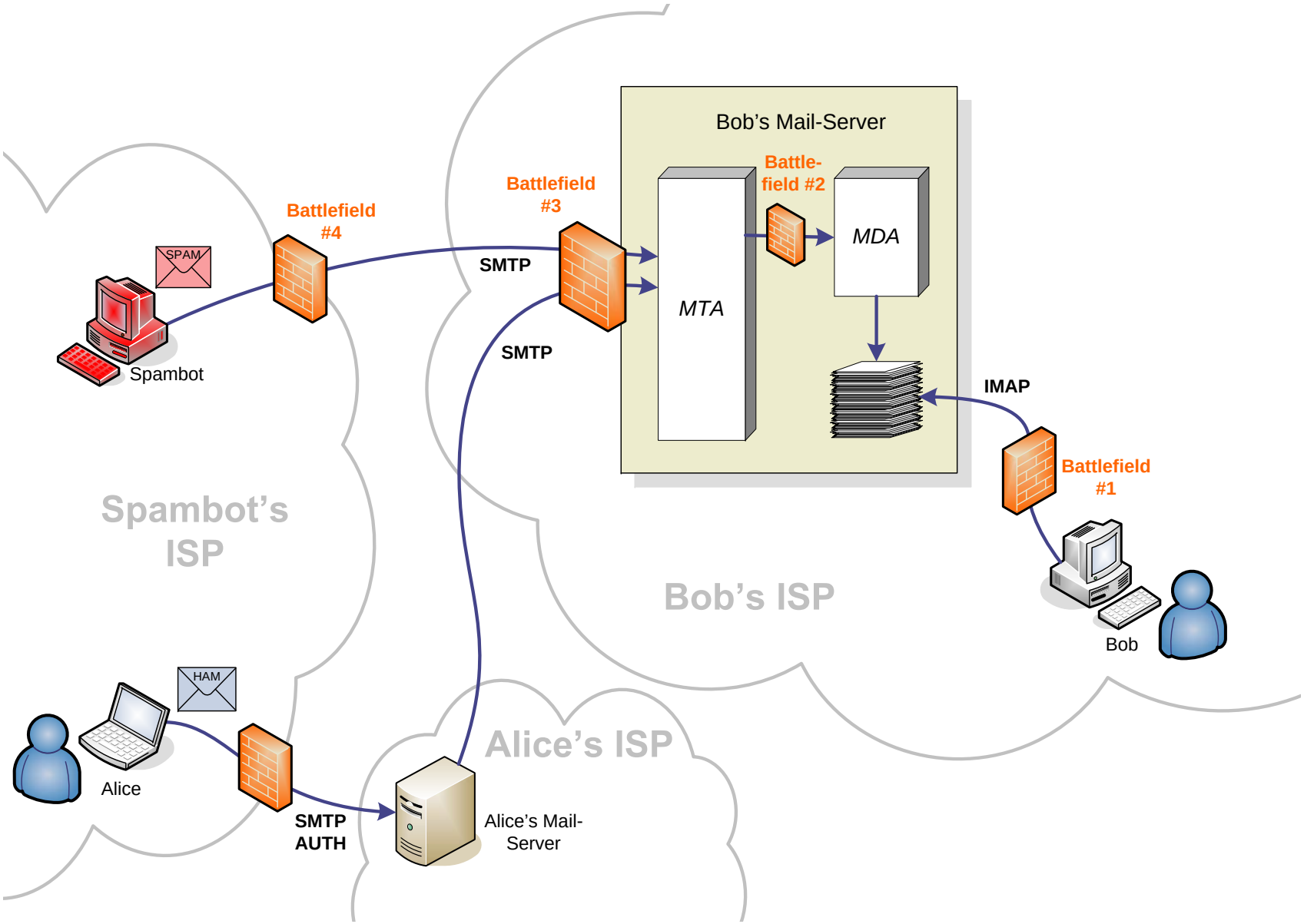
Spam-Source: Port 25 Filtering

```
if port == 25
  use SMTP/TLS
else
  use SMTP/SSL
```

Consequence:

- Implement **port 465** too (smtps - SMTP/SSL)
- IANA: `urd 465/tcp URL Rendesvous Directory for SSM`

Questions?


Bob's Mail-Server
Battlefield #3
Battle-field #2
MDA
MTA
Battlefield #4
SPAM
SMTP
SMTP
Spambot
IMAP
Battlefield #1
Spambot's ISP
Bob's ISP
Bob
HAM
Alice
Alice's ISP
SMTP AUTH
Alice's Mail-Server