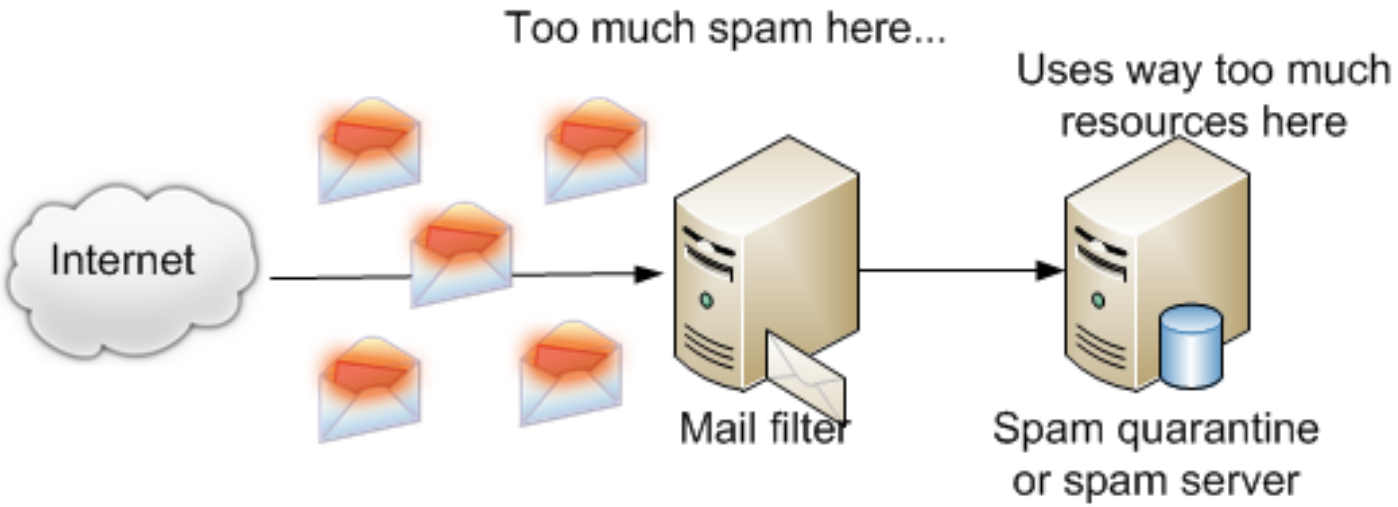
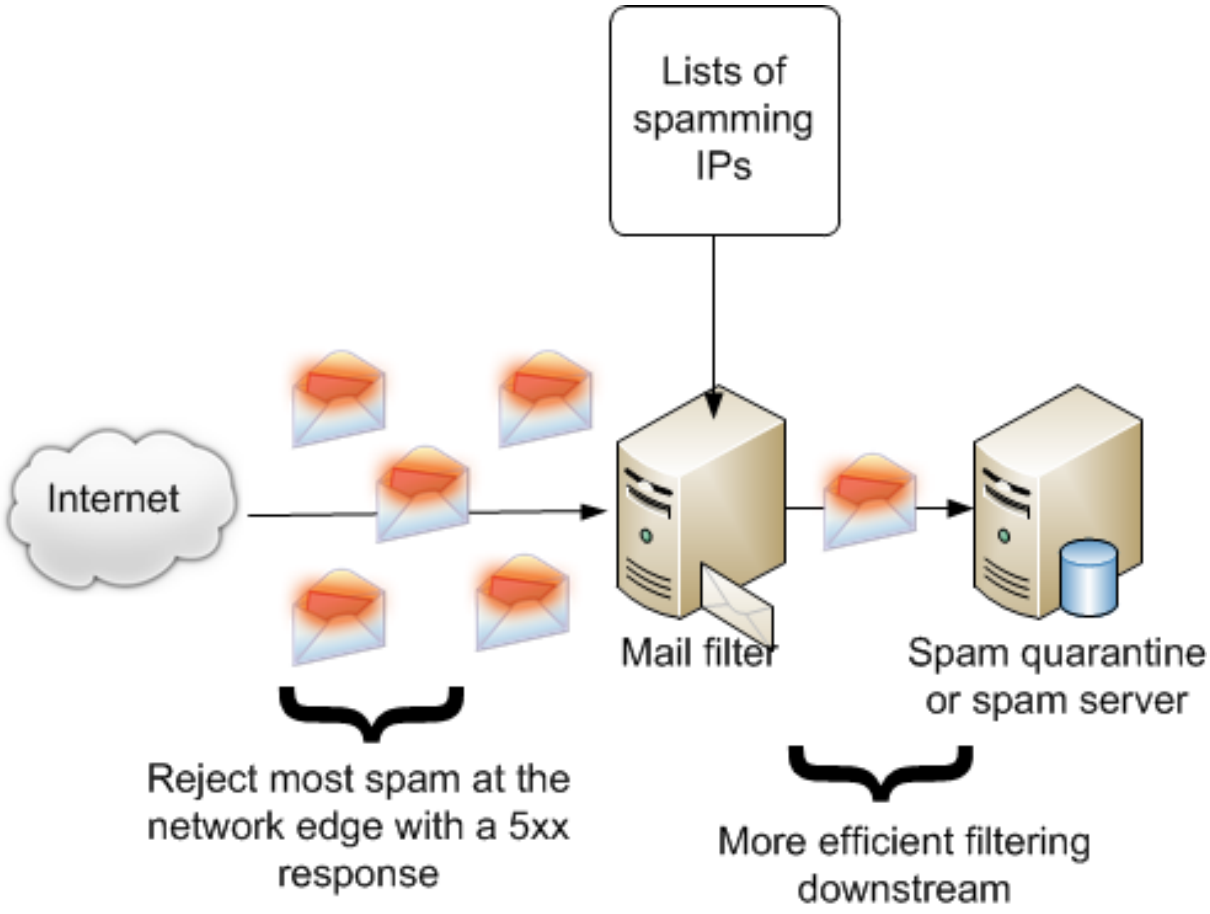
The problem of email spam from IPv6



Modern filters



The problem of scale

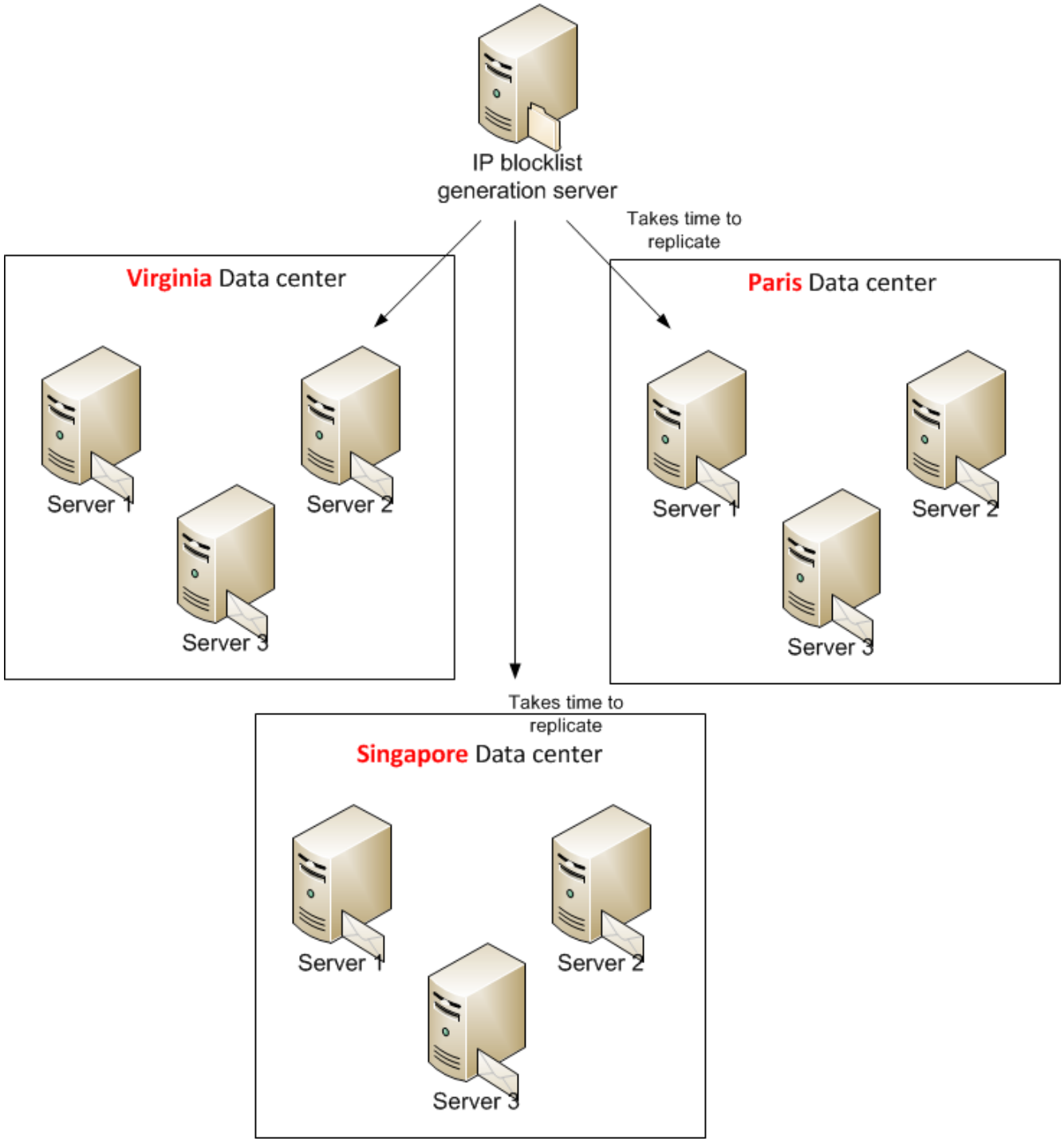
- IP lists must be updated in (near) real time
- Max IPv4 addresses ~ 4 billion
- Max IPv6 addresses ~ 18×10^{38}
  - Even if everyone gets their own /64, max addresses = 18×10^{18}

The problem of scale (cont'd)

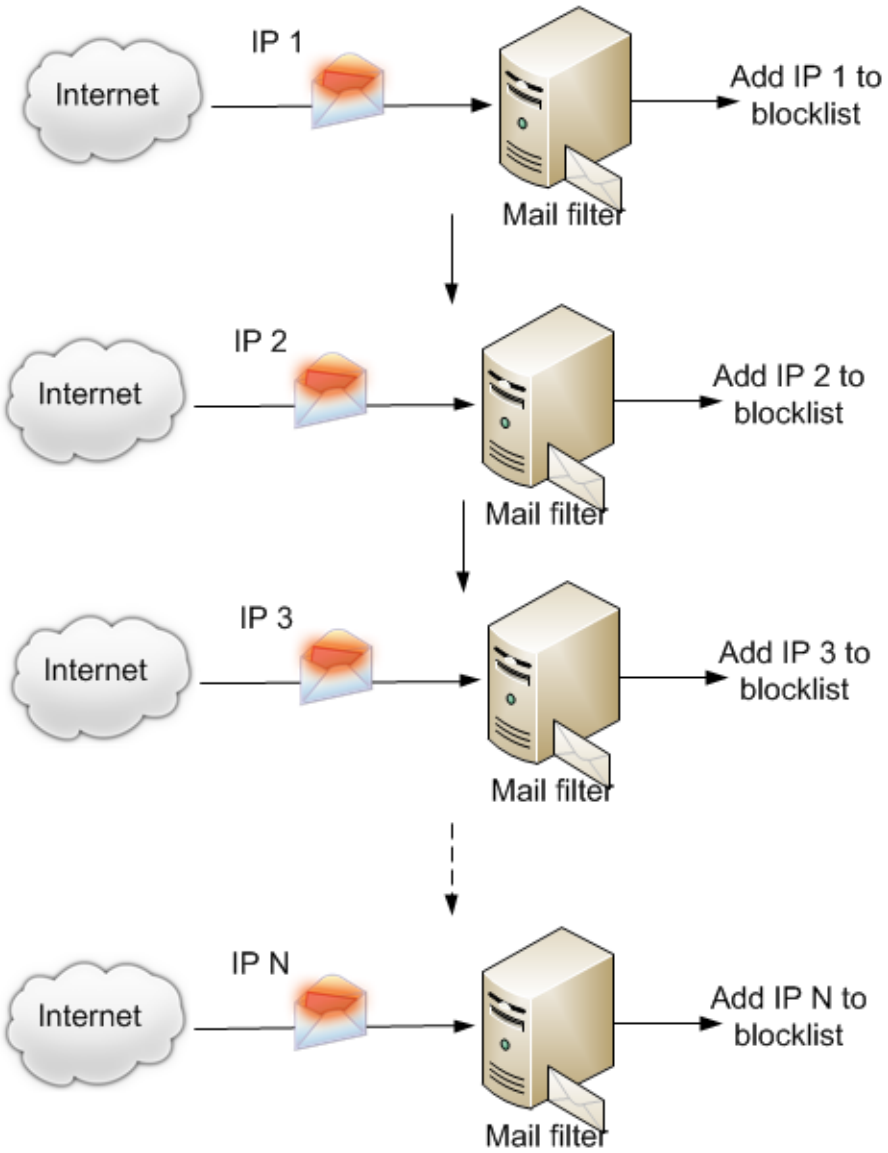
- What happens when we build a better spammer?
  - Every spam comes from a unique IP (or limited reuse)
  - 5 billion spamming IPs per day → Size of file = 190 GB (XBL+SBL+PBL = 138 MB)
  - This is too big!

Too big to process

- Geo-distributed systems must replicate across network quickly (large files take too long for real time effectiveness).
- Processing the file takes a long time.
- IP stats history tables (e.g., Microsoft maintains its own IP reputation tables) grows too big for so many unique IPs.

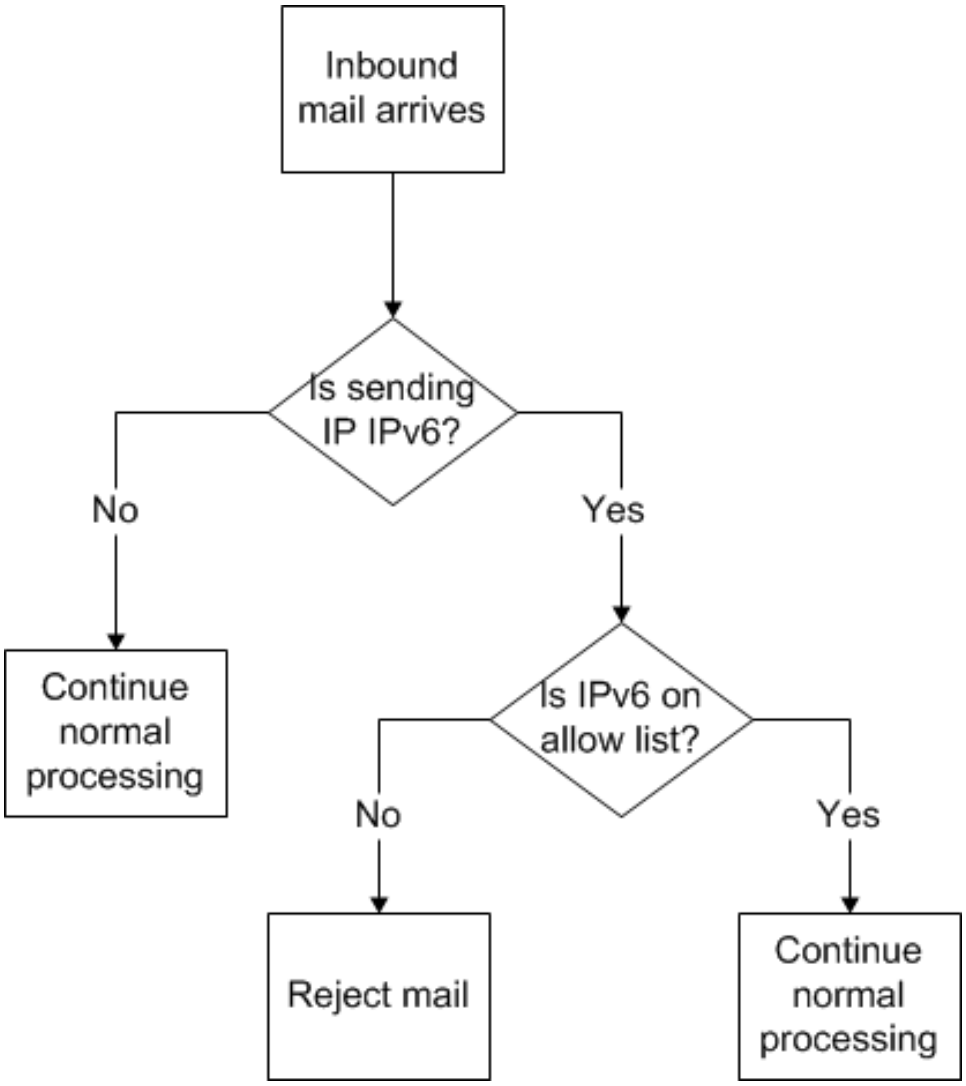

IP blocklist
generation server
Takes time to
replicate
Virginia Data center
Server 1
Server 2
Server 3
Paris Data center
Server 1
Server 2
Server 3
Takes time to
replicate
Singapore Data center
Server 1
Server 2
Server 3

Drop in effectiveness



If spammers don't reuse IP addresses, it makes IP blocklists useless

Proposal (short term) – Allow Lists



Allow List = "I sometimes send legitimate mail over IPv6."

You still perform content filtering.

We already do this for big mailers like Hotmail, Gmail, etc.

Either a central reputation service for IPv6, or build your own.

Do not allow anyone to send you IPv6 email!

Allow lists are ***way*** smaller and easier to maintain.