What does IPv6 mean for delivery?

Why was IPv6 developed?

IPv4 allows for around 4 billion addresses, of which 3.7 billion are usable. This address space is becoming increasingly exhausted. At the end of July 2015 only 160,000 IPv4 addresses were still available to the American Registry for Internet Numbers (ARIN): That represents 0.01% of the total addresses managed by ARIN. IPv6 is a must in order to continue to be able to address the growing number of servers in future.

What impact will IPv6 have on IP reputation?

At the moment ISPs strive to establish a reputation for delivering IPv4 addresses. There are countless external sources which can help in the evaluation of the reputation of an IPv4 address. Particularly favored tools are IPv4 blacklists and whitelists, as they are quite effective. However, the address space created by IPv6 will be so big that spammers will be able to constantly change their IP address and so prevent effective reputation building. The listing of individual IP addresses under IPv6 involves an enormous increase in the size of the list and simultaneously renders the blacklist ineffective, as spammers would never use a single IP address for long.

The only possibility to avoid this problem for an IP-based blacklist is to list networks. The popular and widely available software rbldnsd lists /64 networks in its standard configuration. This usually represents the size of the network that is allotted to a single server. However, IP-based blacklists are still growing exponentially, and the danger of collateral damage correspondingly. The problem does not occur with IPv6-based whitelists. A sender who operates cleanly and is building positive reputation will not voluntarily destroy it by regularly changing its sender server.

IP-based blacklists seem to have hit a dead-end with IPv6. A possible way out is to assume that all incoming IPv6 traffic is bad when the incoming IPv6 address is not already known as a good address. The “warming up” of an IP address would then become much more significant and complex with IPv6 than with IPv4. Alternatively, IPv6 whitelists from trusted sources could also shorten or eliminate a warming-up phase altogether.

How does IPv6 impact on domain reputation?

Another and very practical way out of this dilemma is the development that IP reputation will greatly lose significance and that, instead, domain reputation will become much more important. Probably the greatest advantage of domain reputation for the recipient is the better accuracy possible in spam filters and the possibility to recognize a sender again, even if they are using a different IP address in the meantime (presuming the sender domain does not change).

Emails have to be authenticated in order to establish a domain reputation. SPF and DKIM then become prerequisites, rather than just signs of goodwill and high quality standards.

What else is important?

Regardless of whether IPv4 or IPv6 is being used, the basics still apply:

- Clean technical set-up (e.g. reverse DNS)
- Clean permissions (e.g. DOI, no bought lists)
- List hygiene (handling bounces, handling unsubscriptions and complaints)
- When possible, feedback loops so problems can be identified early.
- Being on a whitelist can massively reduce the warm-up phase and improve delivery

Last, but not least, as behavior-based spam filters are being used more and more, it is not just important to have proper permission and to send emails without any technical issues, but to have relevant content. If the recipient sees the email as being irrelevant or even unwanted, then complaints will increase, even if everything else has been done correctly. Relevant content is more important than ever.

What do I need to do now?

Currently emails are still sent over IPv4. IP reputation is still important for delivery success. Nevertheless, domain reputation is becoming ever more important, even when sending over IPv4 addresses. Depending on the ISP, it can already have a strong influence on delivery. If SPF and DKIM have not yet been implemented then it is high time to do so. DMARC can protect against the abuse of domain reputation. In the coming years, domain reputation will become more and more crucial. Until IP reputation loses significance, if that ever happens, it remains something that needs to be carefully managed.

This means you need to:

- Check whether your own mailing platform and infrastructure is ready for IPv6
- Implement SPF and DKIM, if not already implemented
- Implement DMARC (easy enough when SPF and DKIM have already been implemented)

When the mailing platform is ready for IPv6, when SPF, DKIM, and DMARC have been implemented, and when IP and domain reputation are well managed (e.g. with feedback loops), then all of the technical requirements for delivery have been fulfilled. Now all that is needed is good content.

Authors: Technical Team of the Certified Senders Alliance