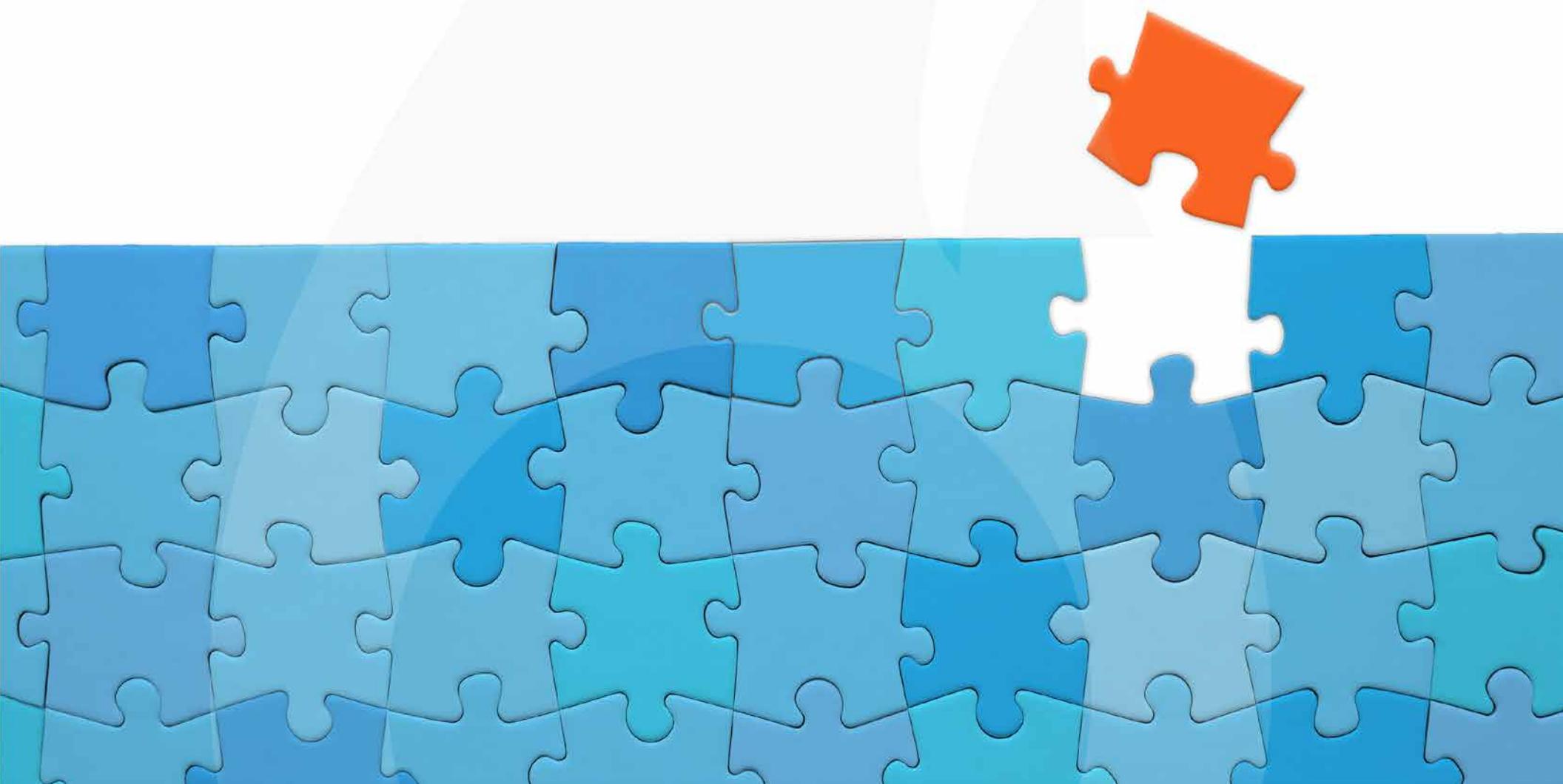


Shared vs Dedicated Email Environments: A Practical Guide



For companies seeking an email solution for their business, there can be a bewildering number of requirements to take into consideration. One of the most important — and often misunderstood — is the question of whether a dedicated IP environment is necessary to ensure deliverability and performance, or if a shared environment will suffice? Whether or not you are considering email services from an ESP (email service provider), or a cloud email service like SparkPost, choosing the right environment can make the difference between succeeding on your own merits, or suffering the consequences of digital guilt by association.

WHY DO I HAVE TO CHOOSE? WHY AREN'T ALL ENVIRONMENTS DEDICATED?

Many email service providers maintain both a shared pool of IP addresses and dedicated or reserved IPs. The first thing you have to understand is that an IP address, in the context of outbound email delivery, is a business commodity and needs to be considered a scarce resource. Think about all you have to muster in order to begin sending from an IP: first you have to obtain it, register it and build up a reputation for it. A shared IP pool can be a more cost effective route to market and allow for companies with limited budgets and resources to take advantage of economies of scale.

¹ Contiguous IPs are right next to each other — IP addresses are classified as part of a network or a range. The most common collection of IPs is referred to as a class C network which contains 255 addresses. Contiguous IPs would be those that follow the sequence, one after another, from .1 through .255. This is a very simple version of the definition of contiguous IPs; for more information you should consult your IT/network expert or this handy guide: <http://www.networkcomputing.com/netdesign/1122ipr2.html>

Understanding Shared IP Environments

A shared IP environment is exactly what it sounds like: a series of IPs, contiguous¹ or non-contiguous, used to send outbound email for a set of emailers that could be part of the same organization or from completely different organizations. Shared IP address pools are probably the oldest and most common way of enabling email for third party senders.

MOST COMMON IMPLEMENTATION

Email service providers are the most common users of shared IP pools and implement them to handle traffic from smaller, inconsistent emailers. As stated before, an IP address is a business commodity and costs money. Additionally, IPs can be monetized, in terms of services and line items that ESPs charge for. A typical shared pool will send out email in a round robin fashion to maximize the overall email load across all of the IPs equally.

WHAT ARE SHARED IPs GOOD FOR?

Typically shared IPs are good for emailers that meet at least one of the following criteria:

- ① Low volume senders that don't have a requirement for a reserved IP because they have no SLAs around delivery times, etc.
- ② Infrequent senders who wouldn't send enough traffic with enough regularity to establish a good email reputation.

A collection of small senders sending email off of a shared set of IPs means that the reputation of that set of IPs will be an aggregate of their individual reputations. Good senders, or those sending email to people who want to receive it

and are actively engaged with the content of those messages (opening, clicking it, filing it away, forwarding it) will find that they may suffer a collateral damage effect where their overall ability to deliver email to the inbox is degraded because other senders using the same IPs have a negative or poor sending reputation. For senders with openly bad practices, or questionable ones, they will actually find they receive a lift in the ability to deliver email because the reputation of the IP will benefit from the good senders whose traffic that IP carries.

The overall effect of a shared IP levels the playing field that brings up poor senders and lowers good ones. *If budget and opportunity exist to use a reserved IP then it should be the desired route to market.* The biggest challenge will be to build up reputation over time and maintain it if the sender doesn't send email frequently enough. Regularly delivered email of smaller sends spread consistently over more days, builds a better reputation faster than large spikes of email with long periods of little to no traffic in between.

WHAT TO LOOK FOR IN A SHARED IP SOLUTION

Shared environments are still widely used by smaller ESPs, transactional email services, marketing automation platforms and others. Most of these companies also offer a dedicated IP service but this often costs money and requires enough volume and traffic to maintain a good emailing reputation. Since not all shared IP pools are alike it's important to make sure you're choosing a service that understands the difficulties in creating and maintaining a shared environment. Some of the things you should look for include:

- A compliance team that carefully screens customers to prevent abusive emailers from taking advantage of the system
- Multi-factor authentication to protect accounts from possible hacking and hijacking.

- 3rd party data highlighting performance
- Excellent documentation to help you understand the platform's operation, the steps taken to protect the shared IP environment and the policies and regulations that establish high quality operating procedures
- A platform that prioritizes transactional email by using a separate set of IP addresses from promotional email. The worst thing imaginable is having transactional email caught behind promotional email in a queue. Delayed password resets, welcome emails, order confirmations, these messages are automated forms of customer service that need to reach their intended recipient quickly and efficiently

Understanding Dedicated IP Environments

Dedicated IPs are the gold standard for how email delivery systems are architected today. Large emailers require a dedicated IP address to ensure they can maintain their own emailing reputation and not suffer the collateral damage of another emailer using that same IP.

WHY WOULD I GO TO THE EXPENSE OF A DEDICATED IP?

The idea that a message stream had to stand out on its own through a dedicated IP evolved due to the blocks levied by mailbox providers who were looking to minimize the abuse detected from shared pools of IPs or IP addresses in the same network. Often it was easier to block an entire class C network, all 255 addresses, vs. each individual IP deemed abusive in a network. By implementing a dedicated IP, you eliminate the risk of having your email negatively affected by other senders on a shared IP address.

MOST COMMON IMPLEMENTATION

The simplest and most common implementation of a dedicated IP is this: two IP addresses, one for all outbound promotional email and a second IP for transactional email. It's very important to separate promotional from transactional email because of the very different natures of these two email streams and how receiving domains regard them. Because transactional messages have minimal (less than 20%) or no promotional content they often have higher deliverability rates. Additionally, having your promotional email blocked is less problematic than having your transactional email blocked which could prevent the delivery of password resets, shipping notifications, order confirmations, etc. When these messages don't arrive, customers often find no other choice but to call support, costing you money, time and resources.

Often emailers with multiple brands under their belt may separate each brand on its own IP address to give them greater transparency into the performance of the brand's individual email stream, content and audience. Because large global organizations leverage distributed teams with distinct responsibilities for a unique brand or geography, the ability to break out the email in a more structured and segmented fashion improves the overall administration of the email infrastructure and transparency in terms of performance.

Very large emailers sometimes opt to have multiple dedicated IP addresses assigned to them by their ESP or from their in-house systems. The logic for a multi-dedicated-IP-address space is based on the idea that:

- ① Spam complaints will be spread over multiple IPs giving an emailer a better overall footprint at a given ISP/emailbox provider.
- ② Some systems have limits on how much email can be sent through a given IP on an hourly basis. Given that certain emailers or brands might have delivery requirements as part of their outbound communications strategy, they may need multiple IPs to accommodate a large delivery and ensure timely deployment.

WHAT ARE DEDICATED IPS GOOD FOR?

Everything. In terms of crisis resolution, triage, etc., dedicated IPs are the fastest road to recovery because you only have to deal with your own IP when attempting to resolve a blacklisting. Dedicated IPs allow you to more easily account for all of your outbound email. It's simpler to discuss your dedicated IPs with an emailbox provider or ISP during crisis resolution if you can affirm the fact that only your traffic goes out over that IP.

Simply put, a dedicated IP infrastructure gives you options — in terms of how you name your IPs, the underlying structure, their authentication records and every other aspect of email-at-scale delivery. Emailers opting to use a dedicated IP should consult their ESP or IT staff to determine the exact throughput they can achieve with their current MTA or emailing solution. Often the limitations of the systems being used will decide if one or multiple addresses are necessary.



A NOTE OF CAUTION.

The act of rotating IPs, a common practice at one time where mail would be switched from IP address to IP address to avoid the fallout of complaints, was and remains a practice associated with spammers. Mailers caught doing this are often penalized and find it even more difficult to deliver to the inbox than if they had solved for whatever problem that originally prevented them from reaching their recipients in the inbox. Switching IPs should be the last option as it requires knowledge, time, resources and patience to re-establish and build a quality sending reputation.

WHEN IPS GO BAD

A bad IP, one that's been abused by senders that may not know better, or actively maligned by spammers, is almost radioactive, a common industry term. The IP address should not be emailed from because there's a long history of abuse

that's been recorded by a variety of receiving domains. The best thing that you can do at this point is stop using the IP, find a new IP and begin building your reputation anew.

WHAT TO LOOK FOR IN A DEDICATED IP SOLUTION

Every ESP on the planet offers dedicated IPs — some transactional email services and cloud email services, like SparkPost Elite, also offer dedicated IPs for customers. Some of the tell tale signs of a well managed and allocated, dedicated IP schema include:

- A team that custom tailors IP addresses, the DNS records and email authentication records based on your business needs.
- A warm-up plan based on real email traffic building reputation over time to prepare for full scale email deployment.
- A ramp up process increasing traffic incrementally while monitoring reputation, bounces, feedback loop complaints and other signals to ensure that a positive reputation is developed on the IPs.
- Automated monitoring tools.
- Automated delivery tools that adjust throughput and throttle by domain giving your email the best chance of success.

- Unique IP addresses for promotional vs. transactional email.
- Unique IP addresses designed to differentiate different brands, lines of business or message streams within your organization.
- A disaster recovery plan for IPs that land on a blacklist.

All senders on the SparkPost Elite email service are architected to send from dedicated IP addresses. Users of SparkPost have the option to use the existing, shared pool or upgrade to a dedicated IP address.

ABOUT SPARKPOST

SparkPost is the cloud solution from the world's number one email infrastructure provider, whose customers — including Facebook, LinkedIn, Twitter, Groupon, Salesforce, Marketo, Pinterest, Zillow and Comcast — send over 3 trillion messages a year, over 25% of the world's legitimate email. Our service outperforms every other cloud or on-premises alternative, and these companies choose us to provide the deliverability, speed and insight they need to drive customer engagement for their business.

 **Improve Your Inbox Deliverability Today.**
Follow us on Twitter [@sparkpost](#) or go to [sparkpost.com](#)