

The 8eI Guide to Changing IP Addressing

This document details the steps required to move to an 8eI supplied public IP address range, either when becoming an 8eI customer or moving as an existing customer to 8eI's ISP service.

Introduction

Any organisation with an Internet connection will have a unique public IP address or range of addresses, so that data they request from the Internet can be routed back to them.

These IP addresses are centrally allocated and managed, and there are currently a limited number of them remaining. IP addresses are allocated to ISP's by the Regional Internet Registry as one IP address range. This range is broken down further into smaller subnets and allocated to end users based on requirements.

Routers on the Internet will contain a route for the ISP's overall address range, which is why ownership of the IPs remain with the ISPs. The end user must "give back" their range of IPs and obtain a new one if they change to a different ISP.

In rare cases, very large organisations may apply for a range of IPs that are independent of a provider (Provider Independent or PI) and can therefore remain with them indefinitely.

Process

The first step in moving to a new range is to identify current and future requirements and submit a request for the required IP allocation.

ISP's are required to justify the subnetting of their IP address range to the Regional Internet Registry who allocated the range in the first instance. The Regional Internet Registry for the EMEA is RIPE. IPs are allocated in blocks of 8, 16, 32, 64, 128, and 256. Larger allocations are available, but due to the limited number of IPs overall, are much more difficult to approve as are allocations of 64 or above.

Organisations are asked to detail their current requirement and how much they expect this to grow within two years. This information is requested via the 8eI RIPE Form. It is expected that organisations will make every effort to minimise their use of public IPs by privately addressing their networks and using Network Address Translation (NAT). 8eI are happy to advise on this if required.

On receipt of the 8eI RIPE Form, 8eI will submit an application to RIPE seeking approval for the requested subnet. Once approved, the IP address range is allocated to the end user and relevant information is entered into the RIPE database. Ideally this will be done in advance of any actual move thereby enabling the organisation to properly plan the migration.

The next step is preparation for changing from one address range to another. The main areas of interest are DNS, Firewall NAT rules, and any connections made referencing IP address only.

Most information accessed over the Internet is done using an easy to remember hostname.

In most cases, the actual public IP addresses are not used directly by anyone accessing an organisation from outside as they are resolved to from hostnames through DNS. In other words, an organisation will have a domain name and will create hostnames using that domain name that resolve to an IP address.

For example, users accessing an organisation's web site will enter a URL, which is simply a hostname, such as www.domain.co.uk. That hostname is resolved by DNS to an IP address, which then leads to the web server itself. Similarly, inbound mail is routed using MX records, which are also hostnames, and therefore resolve to an IP address.

Therefore, in order to change the IP address of the servers, all that needs changing is the DNS zone file for the organisation's domain(s) so that the relevant hostnames resolve to the new IP addresses.

The nature of DNS however, means that it takes up to 24 hours for these changes to propagate throughout the Internet, which means that access to web servers may be difficult during that time, and mail may be rejected until the propagation is complete. Unless it is possible to run both the old and new IPs in parallel if there is an overlap of service provision, there are two ways of dealing with this:

1. Arrange for the changeover to take place during a quiet period. For example, scheduling a change for late on a Friday would have least impact on an organisation's business. Also, *8eI* are able to offer a mail store and forward service that could be configured beforehand to receive any mail that is not able to be delivered directly. This would at least ensure that mail is simply delayed rather than rejected.
2. If possible, change the Time To Live (TTL) value for the hostnames or entire domain. The TTL determines how long a hostname remains valid on a given DNS server before it must be looked up again. If that TTL is 24 hours, the standard value, and a change is made to the master zone file just after a DNS server has loaded the zone, then the change will not be picked up by that DNS server until it has timed out. The TTL can be changed to a much smaller value, such as 5 minutes so that the time for any change to propagate is kept to a minimum. The TTL must be changed back to the standard 24 hours after the change is complete as shorter TTLs mean much more DNS traffic. Also, the initial change to the TTL is subject to the standard TTL in that it takes up to 24 hours to propagate.

DNS can either be maintained by *8eI* or by a 3rd party. If the DNS is to be maintained by *8eI*, so too will the Domain name in question. A further process is introduced for the registration of Domain names.

Firewalls will need to be reconfigured with one of the public IP's acting as the external interface IP. There may be a variety of NAT rules, mapping internal private addresses to one or more public addresses. Unless a new Firewall is to be introduced, the existing Firewall will likely be in operation until the change over. Therefore no addressing can be changed until the changeover takes place. More advice can be provided by *8eI* on this should it be required.

If there are any external connections that use the public IP addresses, such as VPN users for example, then they will need to be notified of the new IP addressing and when it will take effect. It would be a good opportunity to move these to hostnames at this point to allow more control through DNS in future.

Outbound traffic is generally not affected by a change of IPs, although in some instances external systems may have a security policy that requires access to come from a particular IP address. In this case, the administrator of the external system will need to be informed of the change.

Generally, there are some organisations who adopt an approach of changing and fixing what breaks, but 8eI would recommend a more structured approach to this.

The last part of this document is a checklist to aid planning. 8eI are also able to provide more specific help and will incorporate IP address moves into a project plan if appropriate.

Checklist

Preparation

- Ripe form to customer
- Ripe form returned to 8eI core
- Additional DNS form sent to customer (if required)
- 8eI core allocate address range and update RIPE database
- Domain registration request submitted by 8eI if required (this can take up to 4 weeks)
- Customer requests zone file from current ISP (if required)
- Change of TTL in zone files
- Customer requests tag release if transferring domain name (if required)
- Customer notifies 8eI of DNS IP allocation from the new 8eI provided range (if required)
- 8eI to be notified of firewall reconfiguration timescales
- Swap over time to be arranged

Changeover

- 8eI core cabling to be completed
- Customer firewall changes to be made and core physical infrastructure changed over
- 8eI/customer updates DNS records
- Test

Post-change

- Change TTL back to standard if required