What is VLAN Migration and How Does it Affect You?

VLAN, or virtual local area network, is a logically segmented network that can only be accessed by your server(s). All new servers are deployed onto a client specific VLAN, with IPs that can only be used by other servers on that VLAN.

RIR, short for Regional Internet Registry, is responsible for allocating and assigning Internet resources like IP addresses. HostDime strives to use the space allocated to us by RIR in the most efficient and safe format. This includes migrating some clients servers to a private VLAN in our state-of-the-art data centers. Not only does this simplify management and reduce risk, it also helps assure future allocations from ARIN so that we can continue to be able to provide IPs to you. If you have been notified of the need for a mandatory switch-over or would like to know more about VLANs, read on.

VLANs allow us to segment clients from other clients providing better privacy and performance. VLANs are required to enhance security and traffic control; to ease network adds, moves, and changes. VLANs also help with DDoS mitigation and current and future IPv6 allocations, while preventing address stealing, broadcast storms caused by other clients being DDoS'ed, and no local packet sniffing.

In order to move this server onto a VLAN, we need to perform an IP migration. IP migration is the migration of servers between locations. This migration should be scheduled for non-business hours. A usual migration takes about 10 to 15 minutes, however it can take up to an hour if unexpected issues arise.

Follow these steps to make this migration as smooth as possible for you and your clients. HostDime will do most of the work for you, and our actions are below, highlighted in orange.

Step 1 CUT-OVER: The server will be brought offline for about 15 minutes in order to add the new range of IPs to the server. The server's old main IP will also be forwarded to the new main IP. Once complete, both old and new IP ranges will be left available for 2 weeks (we can extend this time period if needed) to provide time for updating DNS records.

Step 2 MAPPING: Our network administrators will provide a mapping of old IPs to new IPs via ticket so you know which IPs need to be changed, where they need to be changed, and what they must be changed to.

Step 3 UPDATES: During the 2 week transitional period, you will need to route all accounts using the old IPs to the new IPs by updating DNS records at yours and your clients' registrar(s), and in any other sensitive locations.

- If all of your clients are using your custom nameservers (ns1.yourdomain.com and ns2.yourdomain.com) then you can make a single change to the glue records at the registrar for 'yourdomain.com' to point those nameservers to the new IP. This will tell your registrar that your nameserver IPs have changed. Your clients using these custom nameservers will not need to make any changes on their end to point their domain(s) to the new IPs.

- If any of your clients are using their own custom nameservers (ns1.theirdomain.com and ns1.theirdomain.com), or the nameservers provided by their registrar (n1.domaincontrol.com and ns2.domaincontrol.com) and pointing the A record to your old IP, they will need to update the old IP to the new IP themselves at their own registrar.

- Any clients using an old IP for software configurations, licensing, monitoring, etc, will need to update the old IP to the new IP it's been mapped to.

- Any gateways or API which restrict access based on IP addresses should also be updated with the new main IP for smooth and normal functioning.

- Virtual environments (other than OpenVZ) will also need to have their main IP addresses, netmask, and gateway changed.

Step 4 AUDIT: Once you've confirmed that all the necessary changes have been made, our team will perform an IP audit to see if we're able to find any outliers. If we see no further changes that need to be made, our team will remove the old IPs from your server.

Step 5 CONFIRMATION: You will want to check through yours and your clients' sites to ensure everything is working properly after the old IPs have been removed. Anything that might not have been pointed correctly could stop working, and these should be reported to our team immediately so we can rectify the problem.

Step 6 COMPLETION: After resolving any reported issues, our team will run one last check to make sure everything is in working order on the server and follow up with your before closing the ticket.

Please note that any software you use which does IP verification (cPanel, etc.) will need to have the new main IP licensed. Also, any gateways or API which restrict access based on IP addresses should also be updated with the new main IP for smooth and normal functioning. Lastly, virtual environments (other then OpenVZ) will also need to have their main IP addresses, netmask, and gateway changed.

If you still have questions, don't hesitate to contact our 24/7 support team.

This article was written by Jared Smith, HostDime's Content Strategist, with help from NSO employee Maxwell C. and CRD employee Michael W.