
Subject: venet without IP on host

Posted by [divB](#) on Thu, 17 Feb 2011 23:10:04 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hi,

I got a /29 subnet assigned from my ISP. Although this are 8 IP addresses, I have only 5 left (Broadcast, network and modem take one each). From the 5 left I need one for the router (internal network) and one for an emergency power switch which is directly connected to the internet. The remaining three addresses are DNS, Mail and Webserver which are OpenVZ container on a hardware node.

As you can see, there is no single IP left. Therefore I connected the WAN interface to the hostnode to a bridge (br-wan) but did not assign an IP address. Each public OpenVZ container uses a veth device which in turn is bridged to br-wan. Additionally, the hostnode has the br-lan bridge an some internal OpenVZ container. The hostnode is only reachable with the internal IP.

However, the veth device are causing problems: First, live migration does not work and second, it is a security flaw which is especially important since they are public containers.

Is it somehow possible to use venet interfaces with those containers although the host has no IP on the same network? As mentioned before, there is really no IP left.

Second question: There are containers within different subnets on the same hardware node (the hardware node has multiple interfaces). How does OpenVZ chose the correct interface for each container?

And finally it becomes even worse: In fact my ISP assigned *two* independent /29 subnets which are both on br-wan. With my current setup, I can have containers in both public subnets. Will this stay possible with venet as well?

Thank you very much!

Regards,
divB

Subject: Re: venet without IP on host

Posted by [tomp](#) on Sun, 20 Feb 2011 13:17:44 GMT

[View Forum Message](#) <> [Reply to Message](#)

You may be able to achieve what you want using proxy ARP.

I believe OpenVZ uses proxy ARP anyway in order to publicise the containers on the network.

Have you tried adding an external IP to the container and an internal IP to the host node?

You may have trouble with routing, as the host node is responsible for routing packets from the container. You may have to use device routes if the host cannot access the external gateway.

Thanks
Tom
