

---

Subject: Re: Re: several nics on the hn  
Posted by [Daniel Bauer](#) on Sat, 08 Oct 2011 09:39:25 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hello Timh,

From: "Timh B" <timh@shiwebs.net>  
> On Fri, October 7, 2011 12:46, Daniel Bauer wrote:  
>> It's an really interesting solution. I've to look at the VLAN  
>> technic,  
>> because I've never used it.  
>>  
>> One thing was, that nobody - only the HN - could change the IP for a  
>> CT.  
>> This issue couldn't be solved by VLAN or veth, so I thought to use  
>> venet.  
>>  
>> Now I think I'll prefer the builtin veth technic to solve my problem  
>> right now.  
>>  
>  
> I would also suggest you go this path, configure your "dedicated"  
> hn-nic  
> (for this example, let's say it's eth0) as usual with the ip-address  
> you  
> want.  
>  
> Example (debian):  
> iface eth0 inet static  
> address x.y.z.n  
> netmask x.x.x.0  
> gateway x.y.z.n  
>  
> iface eth1 inet manual  
>  
> iface eth1.100 inet manual  
> vlan\_raw\_device eth0  
>  
> iface eth1.200 inet manual  
> vlan\_raw\_device eth0  
>  
> iface vmbr100 inet manual  
> bridge\_ports eth1.100  
> bridge\_stp off  
> bridge\_fd 0  
>  
> iface vmbr200 inet manual  
> bridge\_ports eth1.200

> bridge\_stp off  
> bridge\_fd 0  
>  
> --  
>  
> Then, when creating your ct's you simple omit the --ipaddress flag on  
> vzctl command and run vzctl <VEID> set --save --netif\_add  
> eth0,,vmbr100  
> and configure "eth0" within the CT.  
>  
> This will put the ct-network in vlan100 on (hn) eth1 (which as you can  
> see, has no ip-address configured) on the bridge vmbr100 as  
> veth<VEID>.0  
> (confirm with "brctl show"). Note: you will have to configure your  
> switch  
> to send the vlan as "tagged" to the eth1 interface.  
>  
> For your security concerns I suggest you look into mac-filtering or  
> maybe  
> check for mismatches between mac and ip addresses you have configured  
> for  
> the CT, the --netif\_add command will generate a mac-address or you can  
> set  
> one manually.  
>  
> The veth<VEID>.0 interface will also show up in the HN and you can do  
> firewalling with something like this;  
>  
> -A OUTPUT -o veth<VEID>.0 -s <IP> -j ACCEPT  
> -A OUTPUT -o veth<VEID>.0 -j DROP  
>  
> (You will have to check the iptables-commands as I wrote them from the  
> top  
> of my head!)

Thanks a lot for this explanation.

Daniel

---