
Subject: Re: [patch 2/6] [Network namespace] Network device sharing by view
Posted by [Herbert Poetzl](#) on Wed, 28 Jun 2006 17:04:15 GMT
[View Forum Message](#) <> [Reply to Message](#)

On Wed, Jun 28, 2006 at 06:19:00PM +0400, Andrey Savochkin wrote:

> Hi Jamal,

>

> On Wed, Jun 28, 2006 at 09:53:23AM -0400, jamal wrote:

> >

> > On Wed, 2006-28-06 at 15:36 +0200, Herbert Poetzl wrote:

> >

> > > note: personally I'm absolutely not against virtualizing

> > > the device names so that each guest can have a separate

> > > name space for devices, but there should be a way to

> > > 'see' _and_ 'identify' the interfaces from outside

> > > (i.e. host or spectator context)

> >

> > Makes sense for the host side to have naming convention tied

> > to the guest. Example as a prefix: guest0-eth0. Would it not

> > be interesting to have the host also manage these interfaces

> > via standard tools like ip or ifconfig etc? i.e if i admin up

> > guest0-eth0, then the user in guest0 will see its eth0 going

> > up.

>

> Seeing guestXX-eth0 interfaces by standard tools has certain

> attractive sides. But it creates a lot of undesired side effects.

which all can be avoided by not using the host
context for that, but a special 'all seeing'
context (as we have in Linux-VServer) which
can see (and probably manipulate) those interfaces
from the 'admin' PoV without entering the guest
context

> For example, ntpd queries all network devices by the same ioctls as
> ifconfig, and creates separate sockets bound to IP addresses of each
> device, which is certainly not desired with namespaces.

applications scanning the interfaces at startup
are broken by design and should probably be
fixed instead of worked around ...

> Or more subtle question: do you want hotplug events to be generated
> when guest0-eth0 interface comes up in the root namespace, and
> standard scripts to try to set some IP address on this interface?..

why not, would it do any harm when the hotplug
scripts on the host would take the appropriate

actions (i.e. do the required config for the guest)
for special guest interfaces?

but now that you mention it, what about hotplug
events inside the guest?

- > In my opinion, the downside of this scheme overweights possible
- > advantages, and I'm personally quite happy with running commands with
- > switched namespace, like
- > vzctl exec guest0 ip addr list
- > vzctl exec guest0 ip link set eth0 up

I do not consider this the best solution, especially
from the security PoV. don't forget you basically
enter the guest and execute arbitrary programs
(which might have been compromised) to do a setup
task you actually want to happen on the host

best,
Herbert

- > and so on.
- >
- > Best regards
- >
- > Andrey