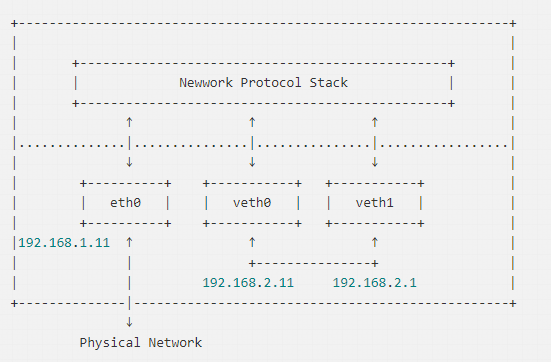
# LINUX虚拟化网络

## Linux虚拟化网络之veth设备

在linux系统中，veth设备模拟成对的网卡接口，veth设备总是成对出现，当一个设备接收到协议栈的数据后，会将数据发送另外一个设备上。

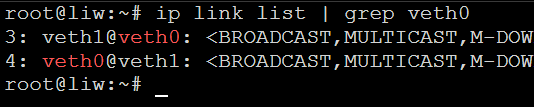


下面通过例子说明veth设备如何使用

1：通过ip link命令添加一个veth设备

ip link add veth0 type veth peer name veth1

2：此时通过ip link可以查看到新增加的设备



3：激活设备

ip link set veth0 up

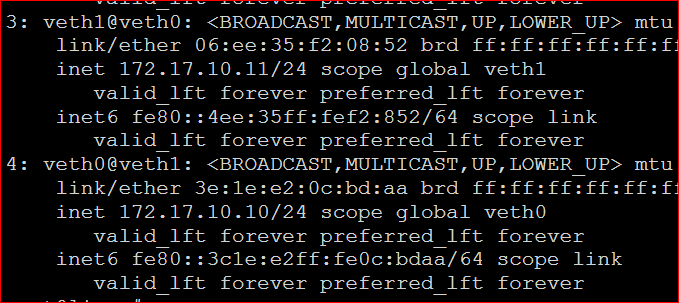
ip link set veth1 up

4：为veth0和veth1配置IP地址

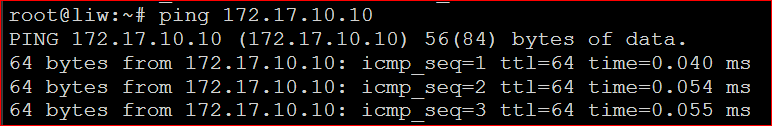
ip addr add 172.17.10.10/24 dev veth0

ip addr add 172.17.10.11/24 dev veth1

5：查看配置的IP地址

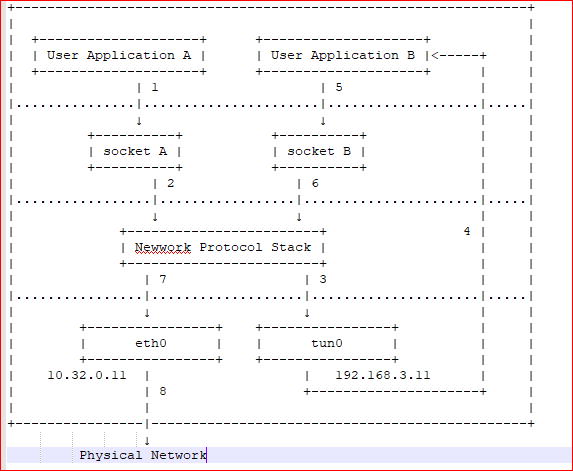


6：使用ping命令互相ping可以ping通



## LINUX虚拟设备tun/tap

Tun/tap是linux下的虚拟网卡设备，该设备一端连接linux内核协议栈，一端连接应用程序。其与普通硬件网卡差别如下图所示：



Tun设备的另外一端是一个应用程序，通常情况下，可以使用tun/tap设备完成vpn工作。

Tun只能支持处理IP层的数据包，Tap设备支持处理链路mac层数据包。

Tun/tap设备使用

使用之前需要安装tunctl命令工具（Ubuntu下可以通过apt install uml-utilities安装）

1：创建一个tap设备

tunctl -t liw-tab

2：为tap设备添加IP地址

ip addr add 172.18.10.10/24 dev liw-tab

3：激活tab设备

ip link set liw-tab up

4：一般场景下，tun/tap设备经常被用于实现vpn，其过程如下

1. 创建一个tun/tap设备，在该设备上配置IP地址等信息，这样，其他应用程序（这里称这些程序为A）将看到一个配置了IP地址的网卡。
2. Vpn程序B打开设备/dev/net/tun，并从该设备上读取数据。
3. 此时A程序发送出的任何数据包，都会被系统送到VPN程序B上，从而B可以对这些数据包进行处理，当B处理完成后，B将打包后的数据包通过真实的网络接口发送到网络上。

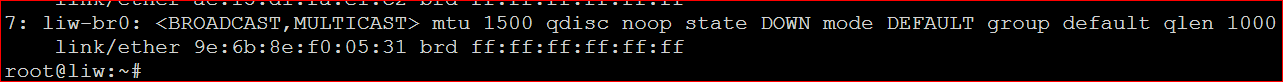
## LINUX虚拟设备虚拟网桥

Linux系统中的bridge可以看作现实网络中的交换机设备，linux-bridge具备网络设备的一切特征，可以有多个端口。

Linux-bridge使用方式如下

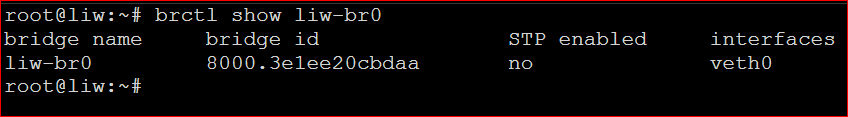
1：在系统中创建也给网桥

可以通过brctl addbr liw-br0命令创建一个名称为liw-br0的网桥设备。



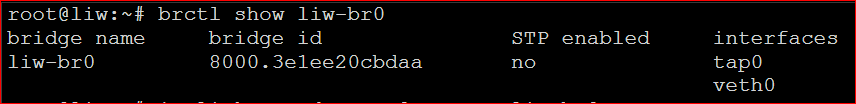
2：可以将veth设备连接到网桥上

ip link set dev veth0 master liw-br0



3：可以将tap设备连接到网桥上

ip link set dev tap0 master liw-br0



此时通过veth1 ping veth0的地址，无法正常访问，此时说明veth0上的ip地址已经无意义，可以删除掉veth0的地址，并将地址配置在bridge上，然后通过ip link set dev liw-br0 up激活网桥设备，此时则可以正常访问veth0的地址。

Linux-bridge常用在如下场景下

1：虚拟机场景下，虚拟机通过tun设备，将虚拟机内的网卡同br0连接起来，这样虚拟机内部发出的数据包，不需要经过host主机的协议栈，从而达到和真实交换机相同的效果。

2：docker场景

处于不同namespace下的容器，通过veth设备将dockers容器内的网卡与bridge连接起来，从而支持dockers内访问外部网络的能力。