???? (networking)

Docker поставляется со следующими сетевыми драйверами в рамках библиотеки libnetwork:

- single-host bridge networks (bridge)
- multi-host overlays (overlay)
- options for plugging into existing VLANs (macvlan)

Для тестов нужно установить

```
apt-get install bridge-utils
```

Docker регистрирует DNS сервис в пределах бриджа. Но в сети по умолчанию (docker0) DNS сервиса нет.

Команда	Описание

brctl show	Список бриджей.
	`sudo brctl show`
	`bridge name bridge id STP enabled interfaces`
	`br-62694f46296d 8000.7ee73b5c2894 no`
	`br-8af5ede4ffdc 8000.aee56ab6b984 no`
	`br-96dd8dcd216d 8000.5a64a8825202 no`
	`docker0 8000.f220300c62b1 no`

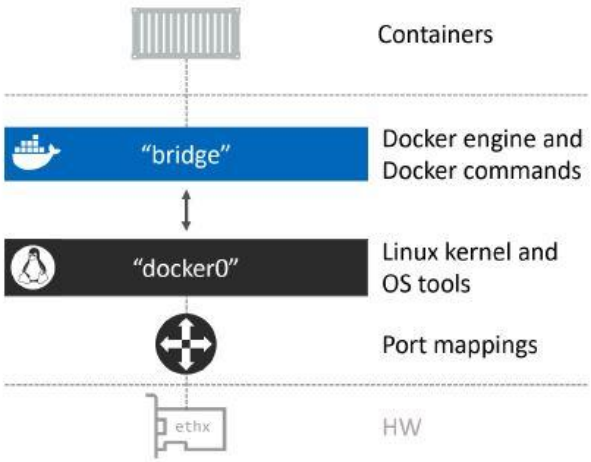
Также есть опция поиска сервисов и балансировка входной нагрузки.

Основная команда	Параметр	Описание
docker network	ls	Список сетей
docker inspect ИмяСети		Выводит информацию по указанной сети. bridge - сеть по умолчанию.

Основная команда	Параметр	Описание
docker network create	-d драйвер	Создает сеть `docker network create -d bridge localnet`
	название сети	
docker port ContName		Выводит map портов внутрь контейнера
docker network prune		Удаляет неиспользуемые сети
docker network rm	Название сети	Удаляет конкретную сеть

Single-host bridge networks

Создается интерфейс на хосте docker.



Один порт может занимать только один контейнер. Взаимодействие контейнеров внутри хоста.

Multi-host overlay networks

Для взаимодействия контейнеров внутри виртуальной сети нескольких хостов. Могут быть расположены на разных нодах swarm. Сеть второго уровня, распределяющаяся по нужным нодам с dns сервисом и распределением нагрузки.

Plugging into existing VLANs

Для прямого подключения к сетевому интерфейсу соответственно с независимым адресом. Необходим promiscuous mode на интерфейсе хоста (неразборчивый режим).

ipvlan с возможностью независимого адреса в пределах диапазона сетевой карты хоста заработал

```
services:
  condb:
    image: nginx
    networks:
      my_ipvlan:
        ipv4_address: 192.168.1.40

networks:
  my_ipvlan:
    driver: ipvlan
    driver_opts:
      parent: enp0s3
      ipvlan_mode: l2
    ipam:
      config:
        - subnet: 192.168.1.0/24
          gateway: 192.168.1.1
```

macvlan напрямую не заработал. Из интернетов:

```
sudo ip link add mymacvlan link enp0s3 type macvlan mode bridge
sudo ip addr add 192.168.1.99/24 dev mymacvlan
sudo ip link set mymacvlan up
```

Docker и firewall

Тут у меня началась веселуха. Первая проблема в том, что в литературе по докеру сетевая подсистема описана слабо, и не говорится самого главного: один хрен ip/nf tables (для определенности далее будем использовать iptables, помня обо всех нюансах). Docker самостоятельно управляет записями в iptables, за счет них организуется сетевая подсистема. Поэтому

1. Все службы вне докера управляются цепочкой INPUT
2. Службы докера, транслируемые наружу (ports в compose файле) по умолчанию попадают в цепочку FORWARD, которая сначала отдает пакеты в цепочку DOCKER-USER, затем в DOCKER-FORWARD и далее блокируется

Цепочка DOCKER-USER служит для пользовательского управления пакетами. Автоматически самим Docker не изменяется. Поэтому в ней можно блокировать например внешние запросы к внутренним сервисам, оставляя доступ для определенных адресов.

Revision #9
Created 17 March 2025 11:25:57 by Admin
Updated 17 August 2025 15:54:09 by Admin