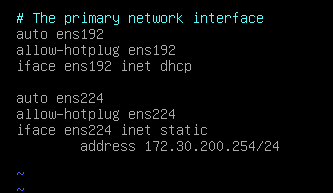
## 8.1 Обзор базовых инфраструктурных и сетевых служб. Пуско-наладка систем кластеризации и контейнеризации.

**IP addressing**

Настройка адресации в Debian

vim /etc/network/interfaces



ifup ens224

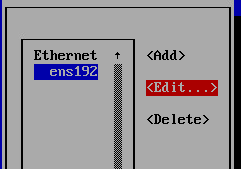
Включение маршрутизации

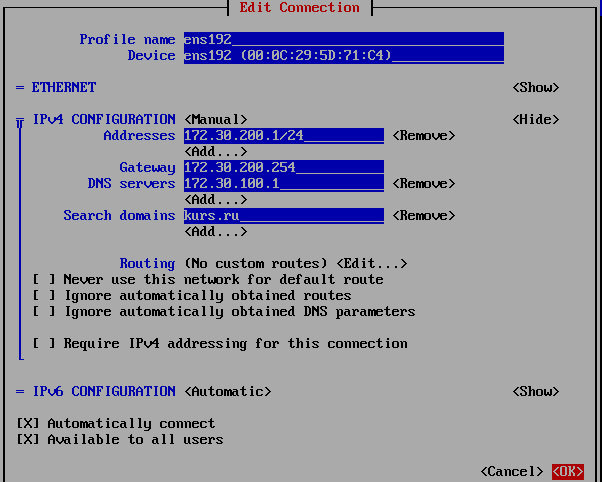
vim /etc/sysctl.conf



sysctl -p

Настройка адресации в CentOS





hostnamectl set-hostname LIN3

nmcli connection modify ens192 \

connection.autoconnect yes \

ipv4.method manual \

ipv4.addresses 172.30.200.2/24 \

ipv4.gateway 172.30.200.1 \

ipv4.dns 172.30.100.1 \

ipv4.dns-search kurs.ru

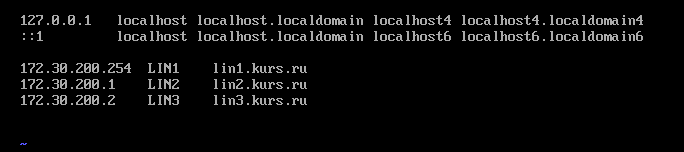
firewall-cmd --change-interface=ens192 --zone=work --permanent

firewall-cmd --zone=work --add-service=glusterfs --permanent

firewall-cmd --reload

firewall-cmd --info-zone=work

vim /etc/hosts

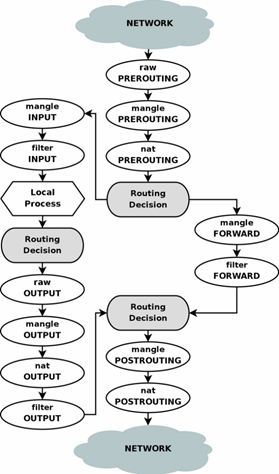


**Netfilter**

Netfilter – это фреймворк, предоставляемый ядром linux, для обеспечения различных операций связанных с сетью.

Netfilter использует таблицы для организации правил. Эти таблицы классифицируют правила согласно типу решения, которое нужно принять. Каждая таблица разделяет правила на цепочки. Грубо говоря, цепочки определяют, когда сработают данные правила.

* Таблица Filter служит для принятия решения о том, стоит позволить пакету продолжить его движение, или отвергнуть его.
* Таблица Raw работает до подсистемы conntrack.
* Таблица NAT используется для реализации трансляции сетевых адресов.
* Таблица Mangle используется для изменения заголовков IP и маркировки пакетов.



iptables — утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter для ядер Linux, начиная с версии 2.4.

Каждое правило содержит **критерий отбора** и **действие,** которое нужно выполнить.

* Критерии
  + Критерии срабатывания L3
    - -i/--in-interface - Входящий интерфейс
    - -o/--out-interface - Исходящий интерфейс
    - -s/--source - Адрес/сеть источника
    - -d/--destination - Адрес/сеть назначения
    - -p/--protocol - Протокол (tcp,udp,icmp, ...)
  + Критерии срабатывания L4
    - --sport port[:port] - порт или диапазон портов источника
    - --dport port[:port] - порт или диапазон портов назначения
* Действия
  + ACCEPT - принять пакет
  + DROP – молча отбросить пакет
  + REJECT- Отбросить пакет и сообщить источнику по icmp
  + MASQUERADE - Source NAT
* Дополнительные модули
  + conntrack/state - критерии срабатывания основанные на состоянии соединения

Подсистема CONNTRACK предоставляет важный механизм отслеживания соединений, на базе которого может происходить фильтрация трафика. Также, этот механизм жизненно необходим для NAT преобразований.

Соединения, отслеживаемые подсистемой CONNTRACK, могут находится в следующих состояниях:

* **NEW**: Новоприбывший пакет, не принадлежащий ни к одному из существующих соединений.
* **ESTABLISHED**: Соединение меняет своё состояние с NEW на ESTABLISHED, когда был получен валидный ответ в обратном направлении. Для TCP это значит, что был получен SYN/ACK, для UDP и ICMP, это значит, что был получен ответный пакет.
* **RELATED**: Пакеты, которые не принадлежат к текущим соединениям, но каким-то образом с ними связаны. Например, ICMP ответы на попытки соединения другими протоколами, или дополнительные соединения FTP.

Документация к iptables

man –k iptables

man iptables

man iptables-extensions

Посмотреть информацию о правилах

iptables -L -v -n --line-numbers

iptables -t nat -L -v -n --line-numbers

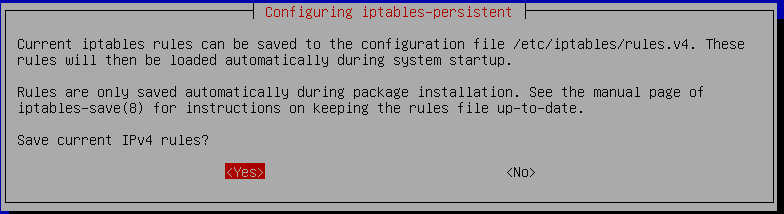
**Настройка NAT**

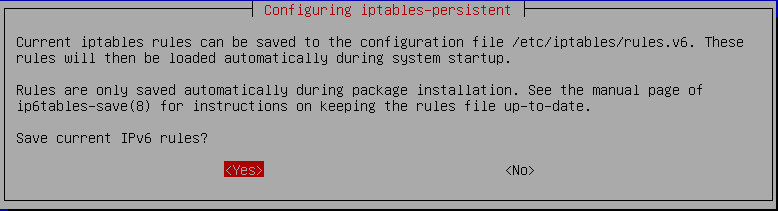
iptables -t nat -A POSTROUTING -o ens192 -j MASQUERADE

iptables -t nat -L -v -n --line-numbers

Сохраняем изменения

apt install iptables-persistent





Сбросить все правила в таблицах filter и nat

iptables -F

iptables -t nat -F

nftables — подсистема ядра Linux, обеспечивающая фильтрацию и классификацию сетевых пакетов/датаграмм/кадров. Является проектом по замене фреймворков iptables, ip6tables, arptables, ebtables в межсетевом экране Netfilter.