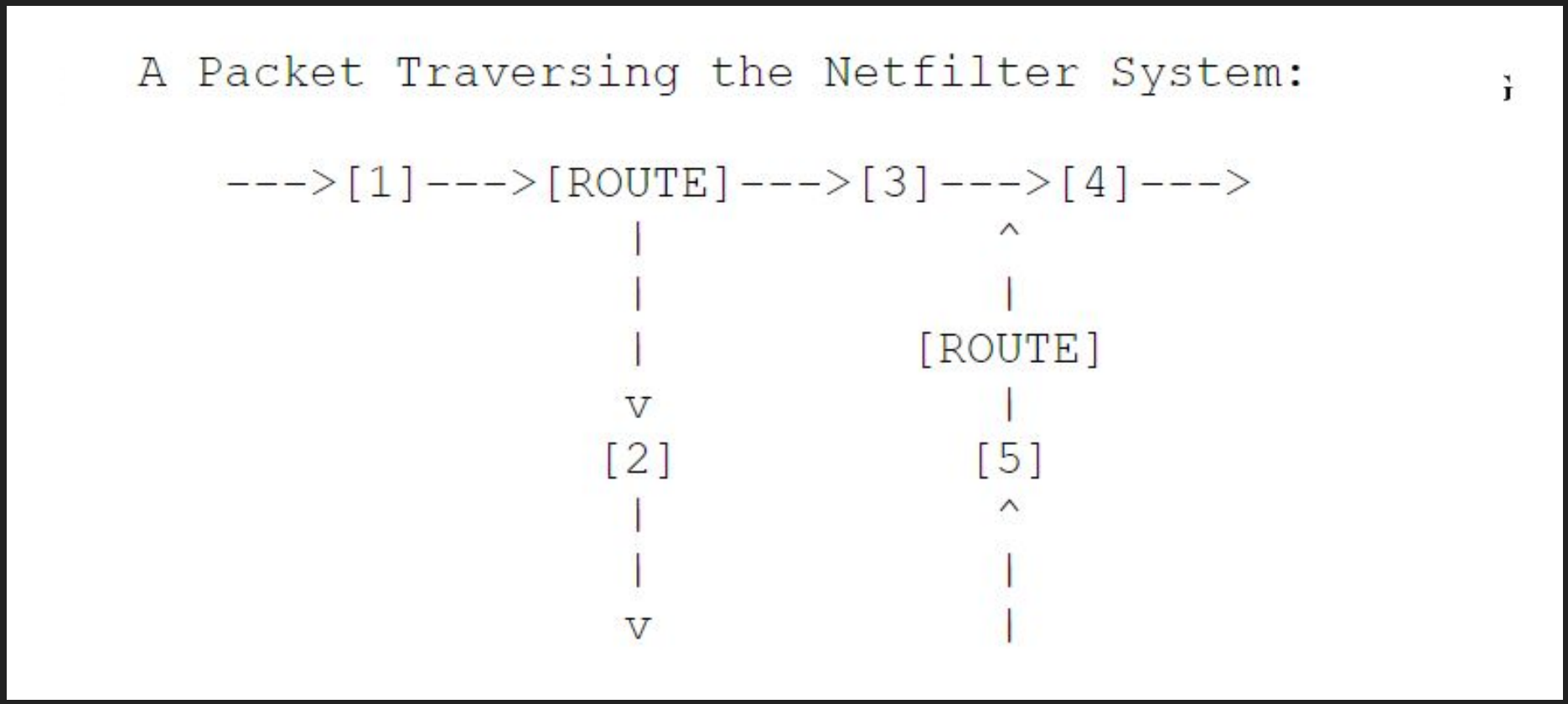
Лекция 11.

iptables

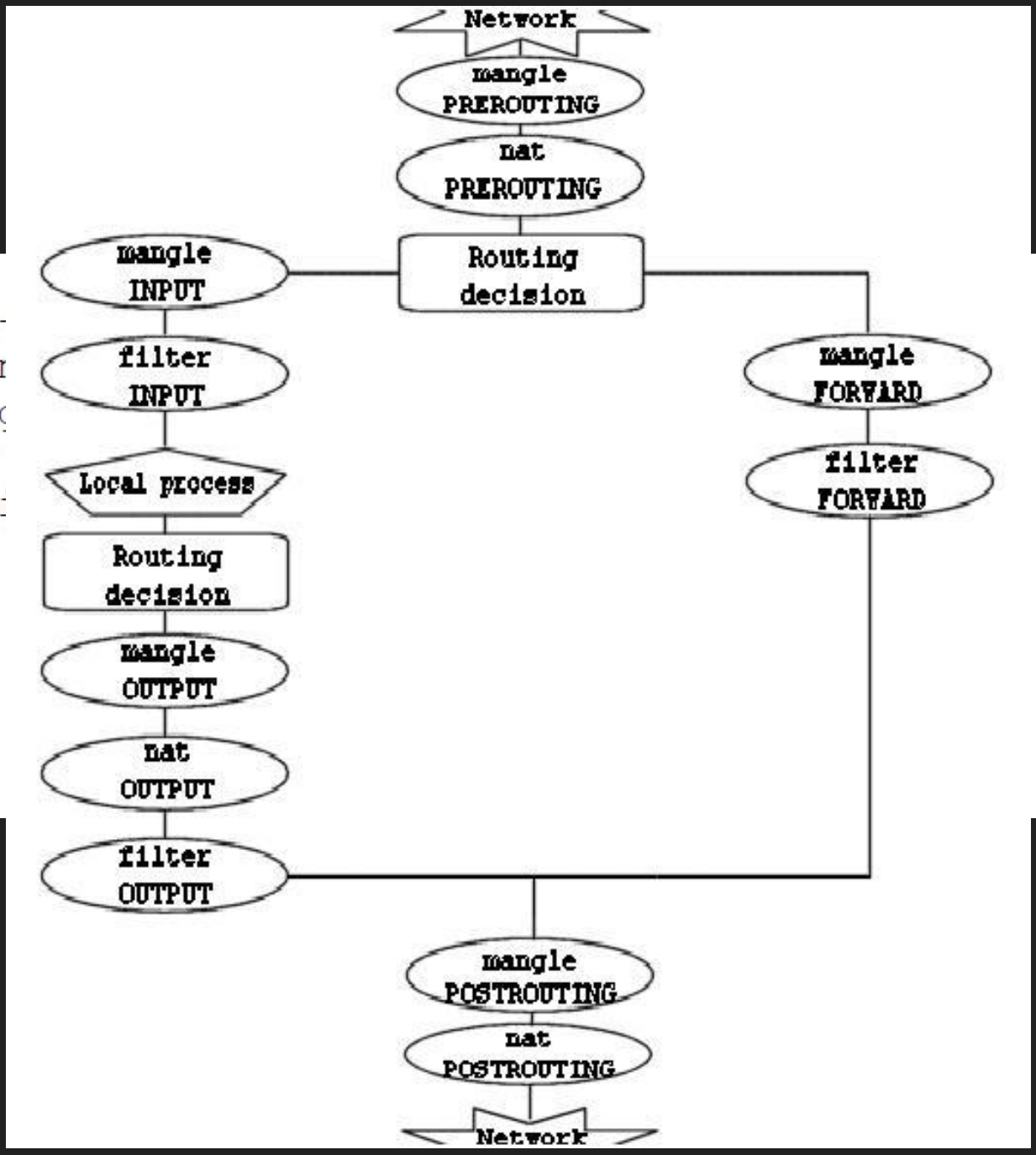
Netfilter


A Packet Traversing the Netfilter System:
--->[1]--->[ROUTE]--->[3]--->[4]--->
[2]
[5]
[ROUTE]

Hooks actions

1. NF_ACCEPT: continue traversal as normal.
2. NF_DROP: drop the packet; don't continue traversal.
3. NF_STOLEN: I've taken over the packet; don't continue traversal.
4. NF_QUEUE: queue the packet (usually for userspace handling).
5. NF_REPEAT: call this hook again.

{ip,nf,arp}tables



iptables

```
linux-intro-qemu:~# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- Netfilter содержит несколько цепочкек:
  - Prerouting – применяются сразу после получения пакета (DNAT)
  - Forward – применяются при маршрутизации пакета
  - Input – применяются перед передачей пакета процессу
  - Output – применяются после формирования пакета процессом
  - Postrouting – применяются перед отправкой в сеть (SNAT, Masquerading)
- Каждая цепочка состоит из таблиц правил:
  - Mangle – правила для модификации заголовков
  - Nat – правила для трансляции адресов
  - Filter – правила для фильтрации пакетов

Iptables: команды

- При вызове программы iptables в первую очередь необходимо указать команду, определяющую действия над таблицей правил
  - -A: Добавить правило в конец цепочки (iptables –A prerouting)
  - -D: удаление правила из цепочки
  - -L: вывод правил в указанной цепочке
  - -F: удаление всех правил из цепочки
  - -N: создание новой цепочки

Iptables: критерии

- При добавлении правила необходимо указать критерии, по которым будет сопоставляться пакет
  - -p: правило для указанного протокола (iptables –A INPUT –p udp)
  - -s, -d: IP адрес отправителя и получателя
  - -sport, -dport: порт отправителя и получателя
  - -m: равенство какого-либо параметра определенному значению
  - --state: пакет в заданном состоянии (iptables –A FORWARD –m state --state NEW)

Iptables: состояния пакетов

- Одним из критерием фильтрации пакета является состояние пакета (--state или --conntrack):
  - NEW – первый пакет для соединения
  - ESTABLISHED – не первый пакет для соединения (получили ответ на первый пакет)
  - RELATED – пакет связанный с уже установленным соединением (все ответы icmp на tcp/udp сообщения)
  - INVALID – пакет не может быть идентифицирован

Iptables: действия

- В каждом правиле необходимо указать действие, выполняемое при выполнении условий фильтрации (-j)
  - Accept – пакет пропускается дальше без какой-либо дополнительной обработки в текущей цепочке
  - Drop – пакет отбрасывается без каких-либо ответов об ошибке
  - Reject – пакет отбрасывается с сообщением об ошибке
  - Dnat – изменить адрес назначения
  - Snat – изменить адрес отправителя
  - Masquerade – то же самое что и snat, только без указания адреса

```
# iptables -A INPUT -p tcp -m tcp –sport 80 -j ACCEPT
# iptables -A OUTPUT -p tcp -m tcp –dport 80 -j ACCEPT
# iptables -P INPUT ACCEPT

# iptables -A INPUT -s 8.8.8.8 -j DROP
# iptables -A INPUT -m iprange --src-range 192.168.0.1-192.168.0.255 -j REJECT
```

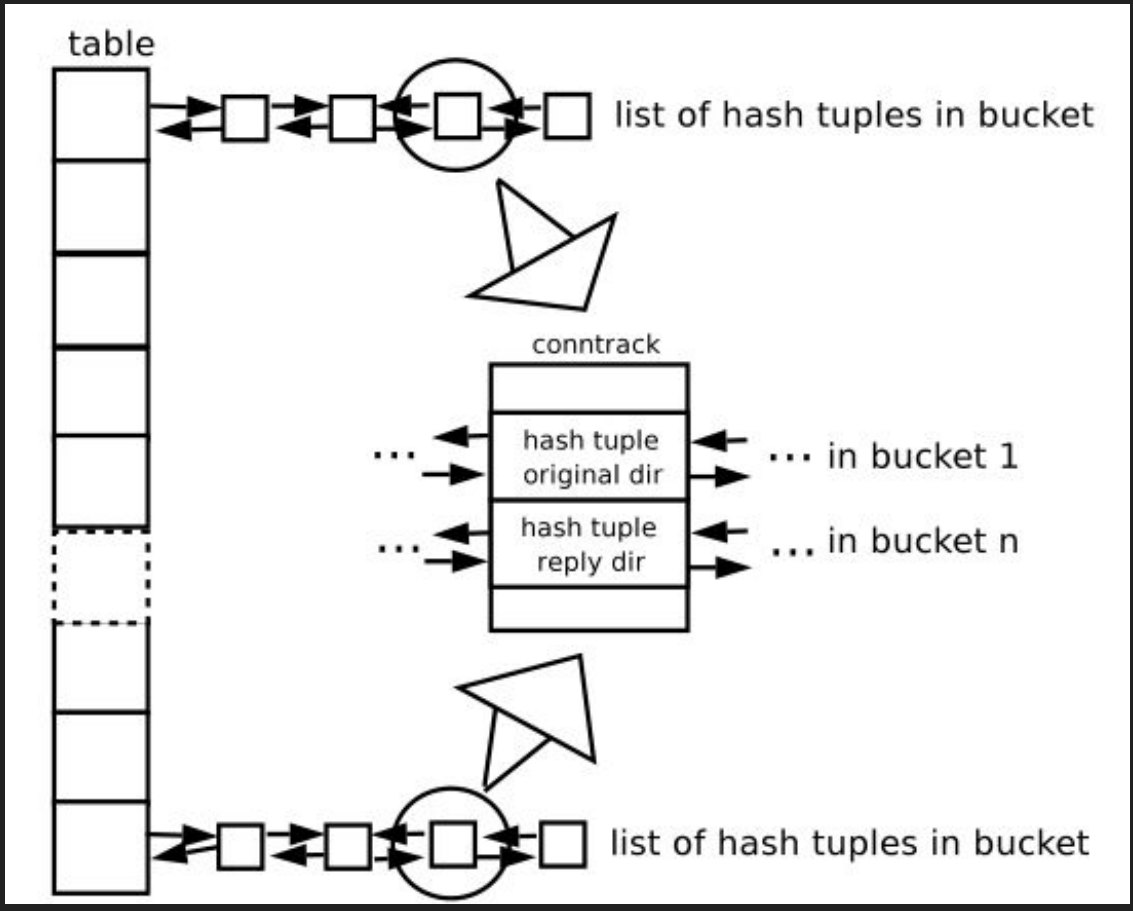
Iptables --help | less

```
iptables v1.8.7

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)

Commands:
Either long or short options are allowed.
  --append  -A chain             Append to chain
  --check   -C chain             Check for the existence of a rule
  --delete  -D chain             Delete matching rule from chain
  --delete  -D chain rulenum
                                 Delete rule rulenum (1 = first) from chain
  --insert  -I chain [rulenum]
                                 Insert in chain as rulenum (default 1=first)
  --replace -R chain rulenum
                                 Replace rule rulenum (1 = first) in chain
  --list    -L [chain [rulenum]]
                                 List the rules in a chain or all chains
  --list-rules -S [chain [rulenum]]
                                 Print the rules in a chain or all chains
  --flush   -F [chain]           Delete all rules in  chain or all chains
  --zero    -Z [chain [rulenum]]
                                 Zero counters in chain or all chains
  --new     -N chain             Create a new user-defined chain
```

nftables_conntrack

- NEW – первый пакет для соединения
- ESTABLISHED – не первый пакет для соединения (получили ответ на первый пакет)
- RELATED – пакет связанный с уже установленным соединением (все ответы icmp на tcp/udp сообщения)
- INVALID – пакет не может быть идентифицирован

```
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```



fail2ban, port knocking

- https://www.fail2ban.org
- https://en.wikipedia.org/wiki/Port_knocking