Факультет
биоинженерии и биоинформатики
Московский государственный университет имени М.В.Ломоносова

Сетевые службы и фильтрация пакетов

Сетевые службы

Network Time Protocol (NTP)

Протокол для синхронизации системного времени.

- 123/udp (иногда и на «клиенте»).
- Иерархическая организация серверов в слои (stratum).
  - Слой 0 – устройства с аппаратными часами высокой точности.
  - Серверы слоя 1 – синхронизующиеся напрямую хотя бы с одним устройством слоя 0.
  - Серверы слоя 2 – синхронизующиеся хотя бы с одним сервером слоя 1.
  - …
- Периодические запросы для сравнения времени с сервером.

Реализации:

- systemd-timesyncd – SNTP-клиент в составе systemd (упрощенная версия протокола NTP).
- ntpd, chronyd – полнофункциональные клиенты+серверы NTP.

Синхронизация времени

SNTP-клиент systemd-timesyncd.service, конфигурация в файле `/etc/systemd/timesyncd.conf`.

```
$ timedatectl
               Local time: Wed 2024-06-05 18:07:04 MSK
           Universal time: Wed 2024-06-05 15:07:04 UTC
                 RTC time: Wed 2024-06-05 15:07:04
                Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no

$ timedatectl timesync-status
       Server: 83.143.51.50 (2.debian.pool.ntp.org)
Poll interval: 34min 8s (min: 32s; max 34min 8s)
         Leap: normal
      Version: 4
      Stratum: 1
    Reference: PPS
    Precision: 1us (-21)
Root distance: 1.174ms (max: 5s)
       Offset: -544us
        Delay: 19.281ms
       Jitter: 2.836ms
 Packet count: 131
    Frequency: +7.977ppm
```

Domain Name System (DNS)

Распределенная иерархическая система для получения информации о интернет-доменах и используемый протокол.

- Доменное имя – человекочитаемый идентификатор компьютера, который можно превратить в IP-адрес с помощью DNS.
- Доменные имена формируют иерархию – полное имя (FQDN) состоит из перечня имен всех вложенных доменов через точку, от листа к корню.
- Каждому домену могут соответствовать записи, его описывающие, в том числе IP-адрес.
- База DNS распределенная – она разделена на зоны (совокупность доменных имен определенного уровня, входящих в домен), за каждую зону отвечает один или несколько DNS-серверов.

Разрешение доменных имен

Реализации протокола DNS:

- встроенный в libc клиент, читает /etc/resolv.conf;
- systemd-resolved – альтернатива в составе systemd;
- BIND – популярная реализация полнофункционального DNS-сервера.

Для разрешения доменного имени программа может:

- использовать функцию из libc – запрос к базе NSS hosts;
- спросить systemd-resolved через D-Bus (org.freedesktop.resolve1);
- использовать собственную реализацию DNS-клиента.

Конфигурация DNS-клиентов

Файл /etc/resolv.conf.

```
# список доменов для поиска коротких имен (без точек)
search fbb.msu.ru fbb.msu
# основной DNS-сервер, IP-адрес или имя
nameserver 192.168.0.1
# альтернативный DNS-сервер (всего допускает до трех строк nameserver)
nameserver 8.8.8.8
```

Традиционно считается системным источником информации о DNS-серверах, используется не только системным DNS-клиентом, но и другими программами.

Системная база имен hosts

Одна из системных баз, настраиваемых с помощью /etc/nsswitch.conf, содержит IP-адреса узлов сети, заданных доменными именами.

```
# /etc/nsswitch.conf
#
...
passwd:         files systemd
group:          files systemd
...

hosts:          files mdns4_minimal [NOTFOUND=return] mymachines dns
...
```

- files – файл /etc/hosts;
- mdns4_minimal – mDNS-клиент (libnss-mdns), только IPv4 и только имена зоны .local, для работы нужен запущенный avahi-daemon;
- mymachines – имена vm и контейнеров через systemd-machined.service;
- dns – DNS-клиент из glibc.

Проверка работы DNS

host – более простая и «дружелюбная» утилита.
dig – «сырая» выдача, удобна для детальной отладки.
nslookup – не использует системную библиотеку DNS-клиента.

```
$ dig '@8.8.8.8' 'fbb.msu.ru' 'MX'
; <<>> DiG 9.16.48-Debian <<>> @8.8.8.8 fbb.msu.ru MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64204
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512

;; QUESTION SECTION:
;fbb.msu.ru.            IN      MX

;; ANSWER SECTION:
fbb.msu.ru.     300     IN      MX  10 kodomo.fbb.msu.ru.

;; Query time: 40 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jun 09 19:39:01 MSK 2024
;; MSG SIZE  rcvd: 62
```

Типы записей DNS

A – IPv4-адрес узла.

AAAA – IPv6-адрес узла.

CNAME – используется для добавления псевдонима к каноническому имени (Canonical NAME).

PTR – указатель (PoinTeR), используется для обратного (reverse) DNS, т. е. определения доменного имени по IP-адресу.

NS – имя DNS-сервера (Name Server), обслуживающего домен.

MX – имя почтового сервера домена (от Mail eXchange).

SOA – Start Of Authority, начальная запись зоны.

TXT – произвольный текст.

Dynamic Host Configuration Protocol (DHCP)

Протокол для автоматической настройки сетевых подключений.

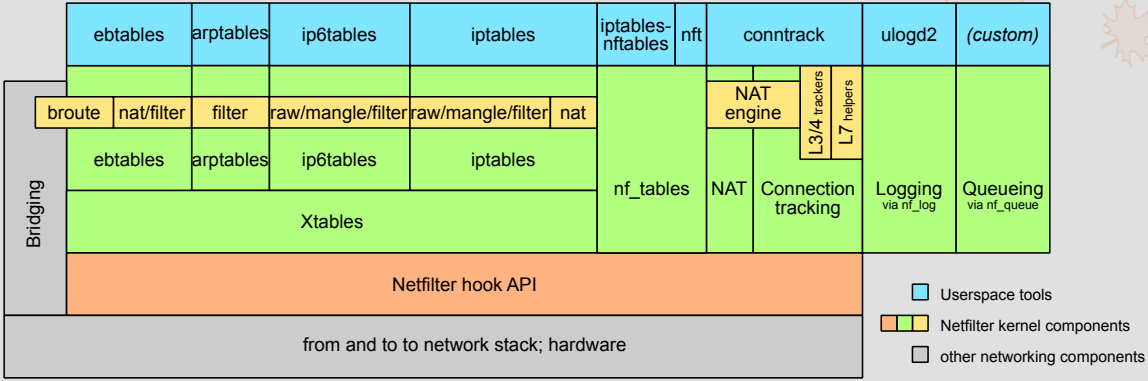
- 67/udp и 68/udp (сервер и клиент).
- Позволяет выдавать клиентам динамические IP из заданного диапазона, или статические (по MAC или другому идентификатору).
- Кроме IP-адреса можно настраивать другие параметры – маску подсети, шлюз по умолчанию, широковещательный адрес, адреса DNS-серверов, имя машины, домен DNS и т.д.

DHCP-клиенты

- isc-dhcp-client (dhclient), ISC прекращает поддержку
- udhcpc – интерфейс для легковесного клиента из busybox
- dhcpcd – альтернативный полнофункциональный клиент
- встроенный клиент systemd-networkd
- встроенный клиент Network Manager
- ...

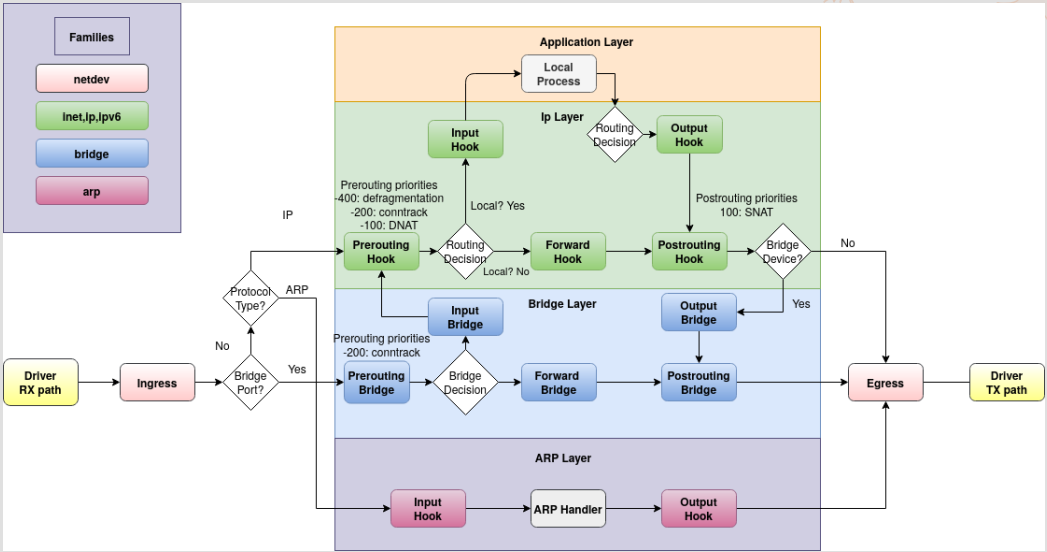
Фильтрация пакетов

Netfilter



based on https://inai.de/images/nf-components.svg by Jan Engelhardt

Путь пакета в ядре Linux



https://wiki.nftables.org/wiki-nftables/index.php/Netfilter_hooks

Устройство nftables

Таблица объединяет цепочки правил, относящиеся к одному семейству адресов:

- **ip/ipv6/inet** – IP разных версий;
- **arp** – ARP-пакеты;
- **bridge** – Ethernet-пакеты внутри мостов;
- **netdev** – Ethernet-пакеты сразу после/до драйвера устройства.

Цепочка объединяет правила, относящиеся к одному этапу существования пакета в ядре. «Базовая» (base) цепочка – привязаная к хуку Netfilter – имеет:

- **type** – что будет происходить с пакетом (filter, route, nat);
- **hook** – к какому nf-хуку привязать;
- **priority** – приоритет цепочки среди привязанных к этому хуку;
- **policy** – что делать с пакетом после прохождения цепочки (accept, drop).

Правило состоит из условий и действий, применяемых к пакетам, удовлетворяющим условиям.

Утилита nft

```
# #показать все правила
# nft list ruleset

# #сбросить все правила
# nft flush ruleset

# #можно вручную добавлять/удалять/изменять таблицы, цепочки и правила
# nft create chain mytab mychain
# nft add chain inet mytab mychain
# nft add rule inet mytab mychain tcp dport http accept
# nft list ruleset
table inet mytab {
        chain mychain {
                tcp dport 80 accept
        }
}

$ #но проще хранить правила в файле-скрипте на языке nft
$ grep -v '^$' '/etc/nftables.conf' | head -n 2
#!/usr/sbin/nft -f
flush ruleset
```

Юнит nftables.service

```
[Unit]
Description=nftables
Documentation=man:nft(8) http://wiki.nftables.org
Wants=network-pre.target
Before=network-pre.target shutdown.target
Conflicts=shutdown.target
DefaultDependencies=no

[Service]
Type=oneshot
RemainAfterExit=yes
StandardInput=null
ProtectSystem=full
ProtectHome=true
ExecStart=/usr/sbin/nft -f /etc/nftables.conf
ExecReload=/usr/sbin/nft -f /etc/nftables.conf
ExecStop=/usr/sbin/nft flush ruleset

[Install]
WantedBy=sysinit.target
```

Противодействие атакам «грубой силой»

Программа fail2ban

- Базовая единица – темница (jail) – состоит из фильтра и действия.
- Фильтр – набор регулярных выражений для поиска ошибок аутентификации в журналах.
- Действие – обычно внесение IP-адреса в список блокировки файервола.
- По прошествии времени блокировки адрес исключается из списка.
- Есть специальная темница recidive для случаев повторных попаданий в список блокировки, для отслеживания таких случаев fail2ban просматривает собственный журнал.

Конфигурация fail2ban

fail2ban.conf – глобальные настройки сервера fail2ban.

filter.d/*.conf – описания фильтров – набор регулярных выражений.

action.d/*.conf – описания действий по блокировке/разблокировке.

jail.conf – описания темниц – указание фильтра, действий и дополнительных параметров (число разрешенных ошибок, время блокировки, ...).

Модификации настроек рекомендуется вносить в аналогичные файлы с расширением .local.

Клиент-серверная архитектура fail2ban

- Серверу fail2ban соответствует юнит fail2ban.service.
- fail2ban-client – позволяет получать и динамически модифицировать настройки во время выполнения и контролировать состояние темниц.

```
# #узнать статус темницы
# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 2
|  |- Total failed: 930
|  `- File list: /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned: 266
   `- Banned IP list: 8.8.8.8

# #разблокировать IP-адрес во всех темницах
# fail2ban-client unban '8.8.8.8'
1

# #узнать время блокировки в темнице sshd в секундах
# fail2ban-client get sshd bantime
1200
```