

Сетевые технологии и протоколы

17.02

Wireshark

- <https://www.wireshark.org/download.html>
- Онлайн, офлайн разбор
- 3000 протоколов
- Расшифровка трафика

The screenshot displays the Wireshark network protocol analyzer interface. The main pane shows a list of captured packets, with the selected packet (No. 1139) expanded to show its details. The details pane is divided into several sections:

- IP: 1139.0.1.10000/v**: Shows the source and destination IP addresses.
- Internet Control Message Protocol (ICMP): Echo (ping) 64 bytes to 1139.0.1.10000/v**: Shows the ICMP Echo request details.
- Application/javascript**: Shows the content type of the request.
- POST /graphql HTTP/1.1/v**: Shows the details of the HTTP POST request, including headers and body.

The selected packet details include:

- POST /graphql HTTP/1.1/v**
 - Connection: keep-alive/v
 - Content-Length: 8202/v
 - sec-ch-ua: "Chromium" v="116", NotA;Brand v="24", "Google Chrome" v="116/v
 - Content-Type: application/json/v
 - sec-ua-mobile: ?v
 - User-Agent: Mozilla/5.0 (Linux; U; X11; en_x86_64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.38/v
 - Origin: http://127.0.0.1:8080/v
 - Sec-Fetch-Site: same-origin/v
 - Sec-Fetch-Mode: cors/v
 - Sec-Fetch-Dest: script/v
 - Referer: http://127.0.0.1:8080/v
 - Accept-Encoding: gzip, deflate, br/v
 - Accept-Language: fa-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7/v
 - Cookie: PHPSESSID=trab684f9e908b171822; securitySystem; SL_WMP_TORUS; SL_WMP_TOS_Hide_Status; SL_wpt1on1api1/v
- [Raw request URI: http://127.0.0.1:8080/graphql/v]**
- [HTTP request 372]**
- [Raw request in Frame: 198]**
- Message in Frame: 1139**
- HTTP Object Notation (application/json)**

Wireshark - фильтры захвата

- `host 172.18.5.4`
- `net 192.168.0.0/24`
- `dst net 192.168.0.0 mask 255.255.255.0`
- `port 53`
- `port not 53 and not arp`

Wireshark – фильтры отображения

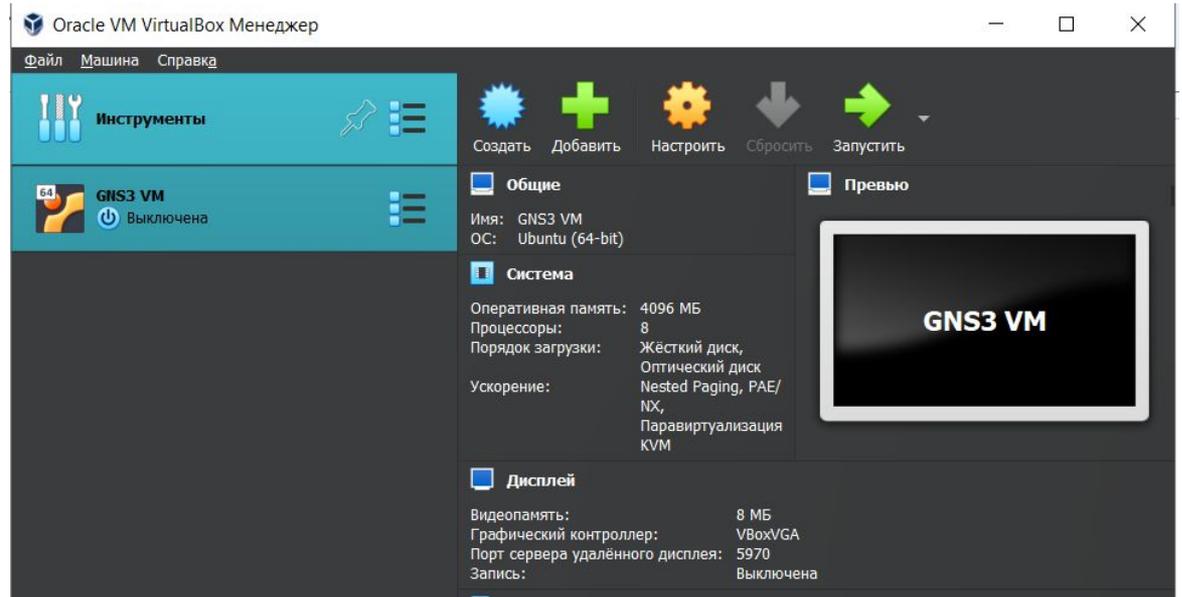
- `ip.addr == 10.43.54.65`
- `ip.dst == 10.43.54.65`
- `ip.addr == 10.43.54.65 and ip.addr == 10.43.54.69`
- `!(ip.addr == 10.43.54.65)`
- `ip.src == 10.43.54.65 and tcp.dstport == 25`
- `tcp`
- `http`
`http.request`

Виртуальный стенд

- Задача: протестировать определенную сетевую технологию.
- Что требуется: n конечных узлов и сетевых устройств
- Проблема: сетевых устройств нет, конечный узел один
- Решение: виртуальный стенд
- Что можно эмулировать:
 - конечных пользователей
 - сетевого оборудования
 - любое сетевое взаимодействие

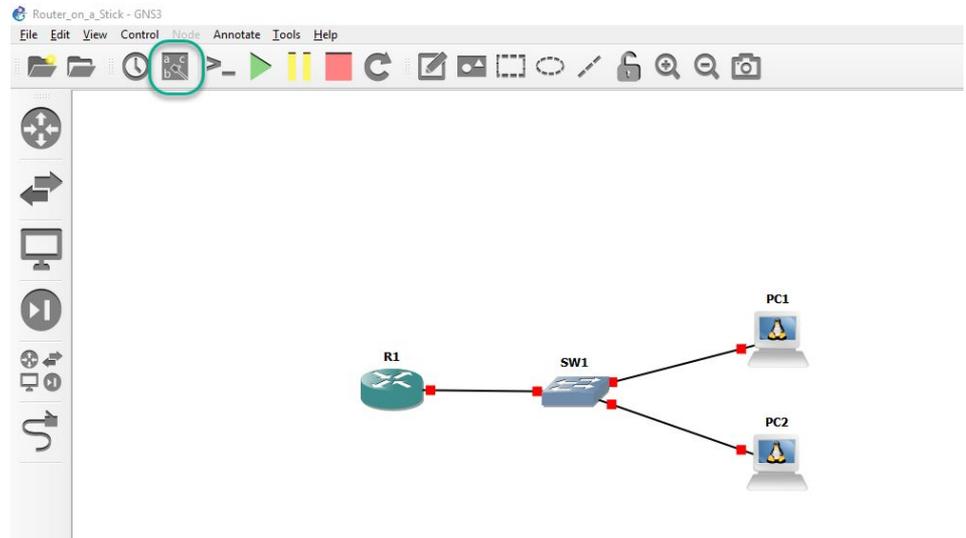
Виртуальные машины

- VirtualBox
- VmWare
- HyperV
- Qemu



GNS3

- Визуализация сетей
- Много поддерживаемых сред виртуализаций
- Простая настройка сетевых конфигураций

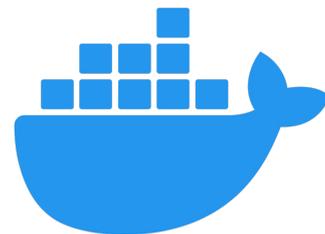


Контейнеры

- Не являются виртуальными машинами
- Позволяют создавать сети из контейнеров
- Контейнеры легче виртуалки (чаще всего)



podman

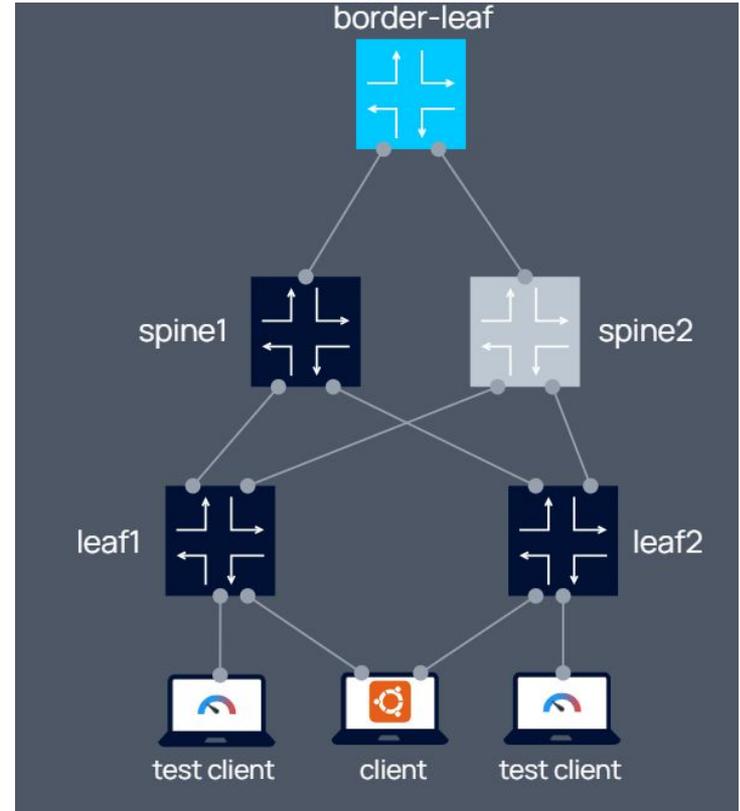


docker

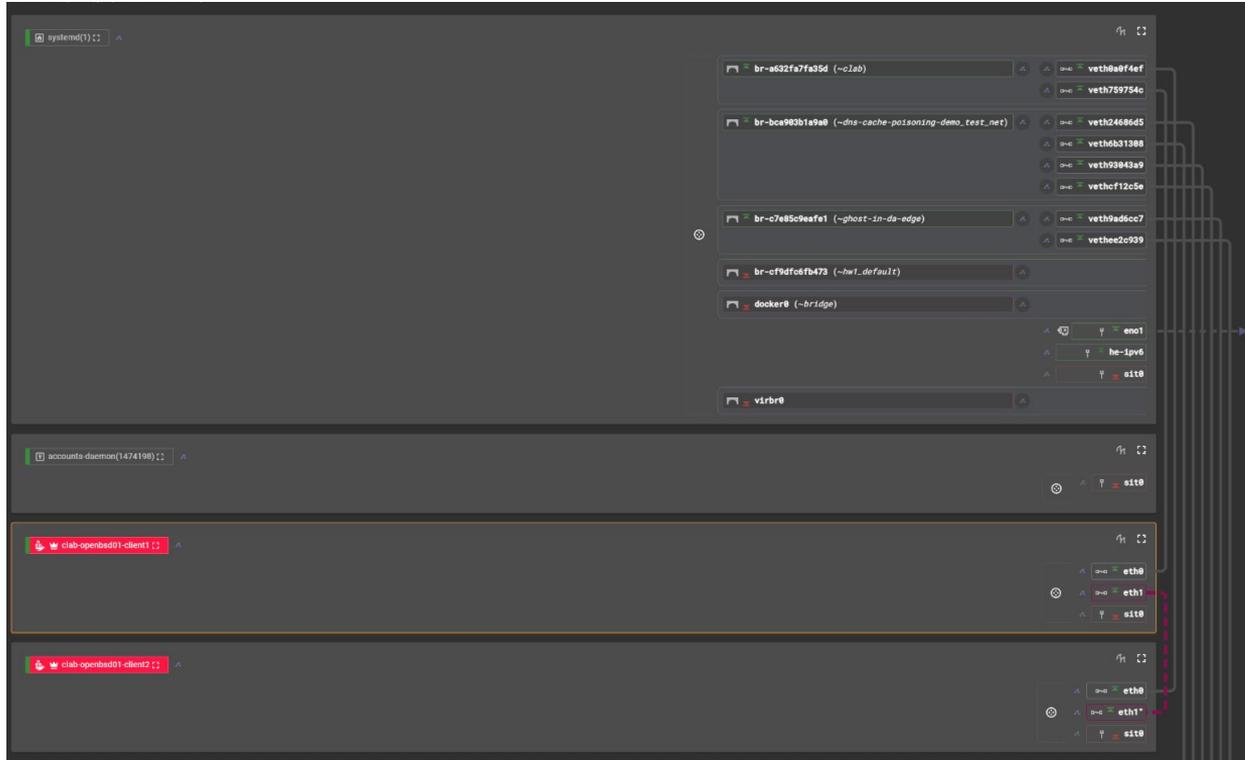
Containerlab

- Работает поверх контейнеров docker
- Описание топологий в yml файлах

```
name: openbsd01
topology:
  nodes:
    client1:
      kind: "linux"
      image: wbitt/network-multitool:alpine-extra
      exec:
        - ip addr add 192.168.1.2/30 dev eth1
    client2:
      kind: "linux"
      image: wbitt/network-multitool:alpine-extra
      exec:
        - ip addr add 192.168.1.1/30 dev eth1
  links:
    - endpoints: [client2:eth1", "client1:eth1"]
```



Edgeshark



Что такое интернет?

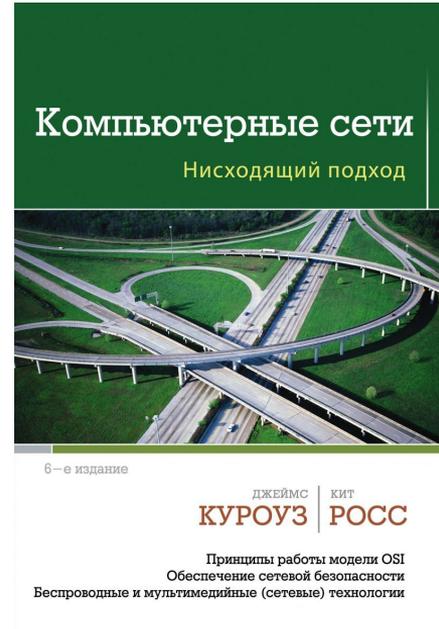
Сеть сетей

Компьютерные сети. Таненбаум, Уэзеролл.



Инфраструктура служб для приложений

Компьютерные сети. Нисходящий подход. Куроуз, Росс.



Еще раз про модель OSI

- Почему в заголовках http нет ip адреса?
- Инкапсуляция, но не ООП

Инкапсуляция

