

netshe_pcap

[Original file](#)

Универсальное программное обеспечение для сетевых устройств NETSHe.

Руководство пользователя

Захват пакетов встроенными средствами для последующего анализа

Станислав Корсаков, ООО «Нетше лаб»

(с) 2009-2020 Ярославль

Встроенное ПО на базе NETSHe может иметь в своем составе средства для захвата пакетов, проходящих через интерфейс и записи захваченных пакетов в файл для последующей загрузки с устройства и анализа в анализаторах типа wireshark.

Воспользоваться средствами можно как из веб-интерфейса, так и из командной строки.

Ограничения и особенности реализации

Средства захвата трафика основаны на утилите tcpdump и унаследовали все особенности и ограничения, свойственные данной утилите.

Кроме того, следует учитывать особенности устройств, на которых работает NETSHe, а именно:

- ограниченную мощность процессора, что может привести к пропуску пакетов и даже потере связи с устройством;
- невозможность записать файл захвата куда-либо, за исключением каталога /tmp (а это оперативная память)
- ограниченный объем оперативной памяти, что может привести к её исчерпанию при длительном захвате в файл.

При разработке данного инструмента, мы исходили из того, что выполнение захвата на устройстве — это элемент отладки и поиска проблем в сетевой конфигурации.

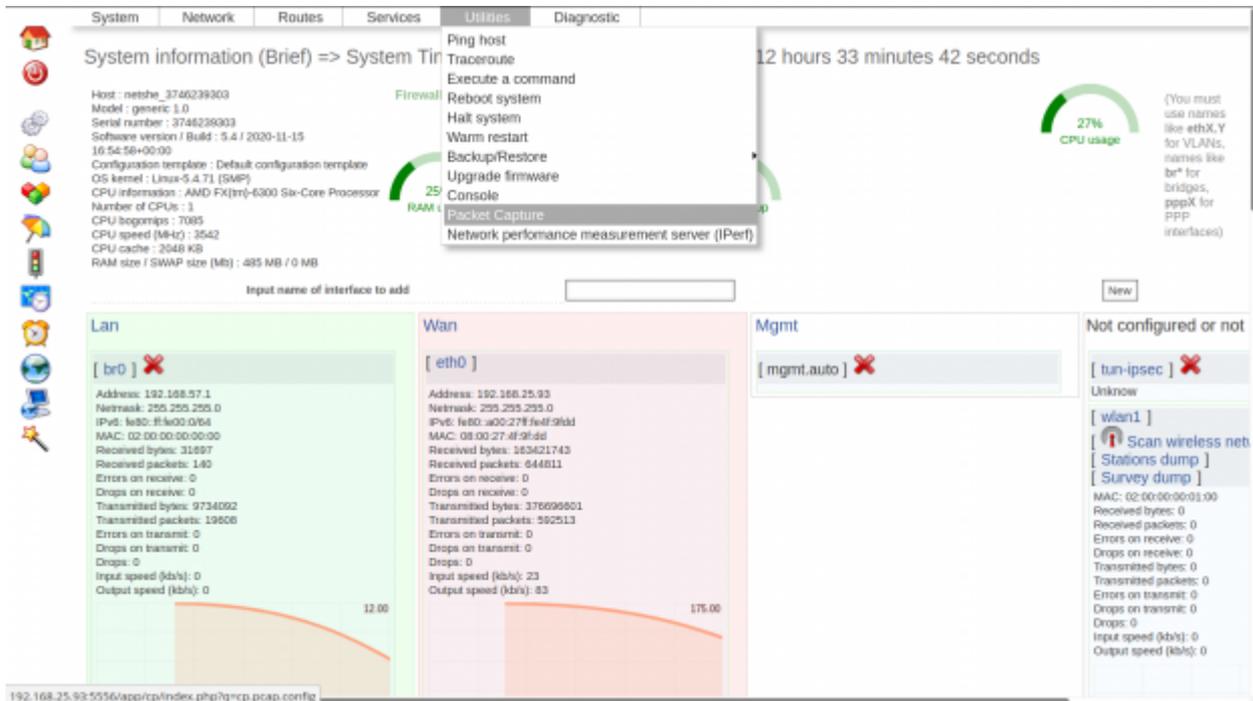
Мы записываем файл захвата в оперативную память и не удаляем его, поскольку считаем, что при завершении отладки/поиска проблемы устройство может быть беспрепятственно перезагружено.

Пожалуйста, не используйте данный инструмент для:

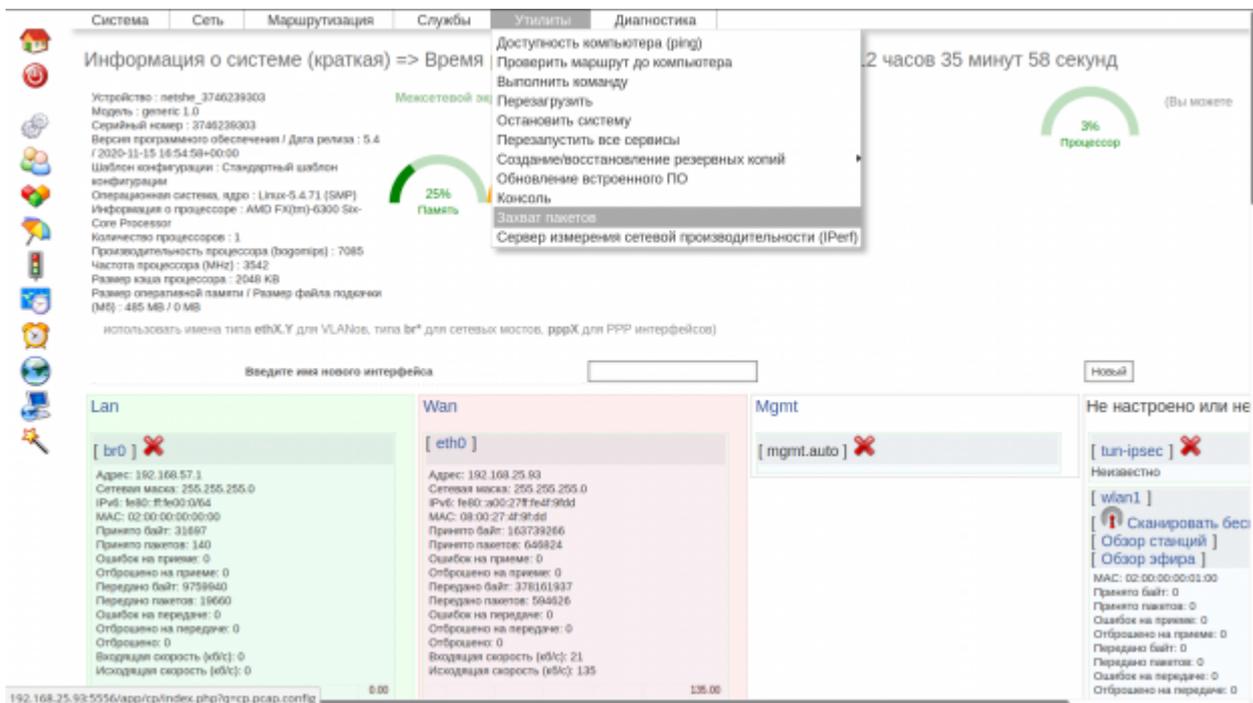
- захвата потоков трафика в десятки Мбит/сек;
- непрерывного захвата трафика в течение часов;
- когда невозможно предсказать объем трафика, который будет захвачен;
- если устройство нельзя перезагрузить после захвата или нельзя удалить файл захвата вручную из консоли, по завершению процедуры.

Захват трафика из веб-интерфейса

Для захвата трафика, выберите пункт меню «Utilities→Packet capture» в англоязычной версии интерфейса

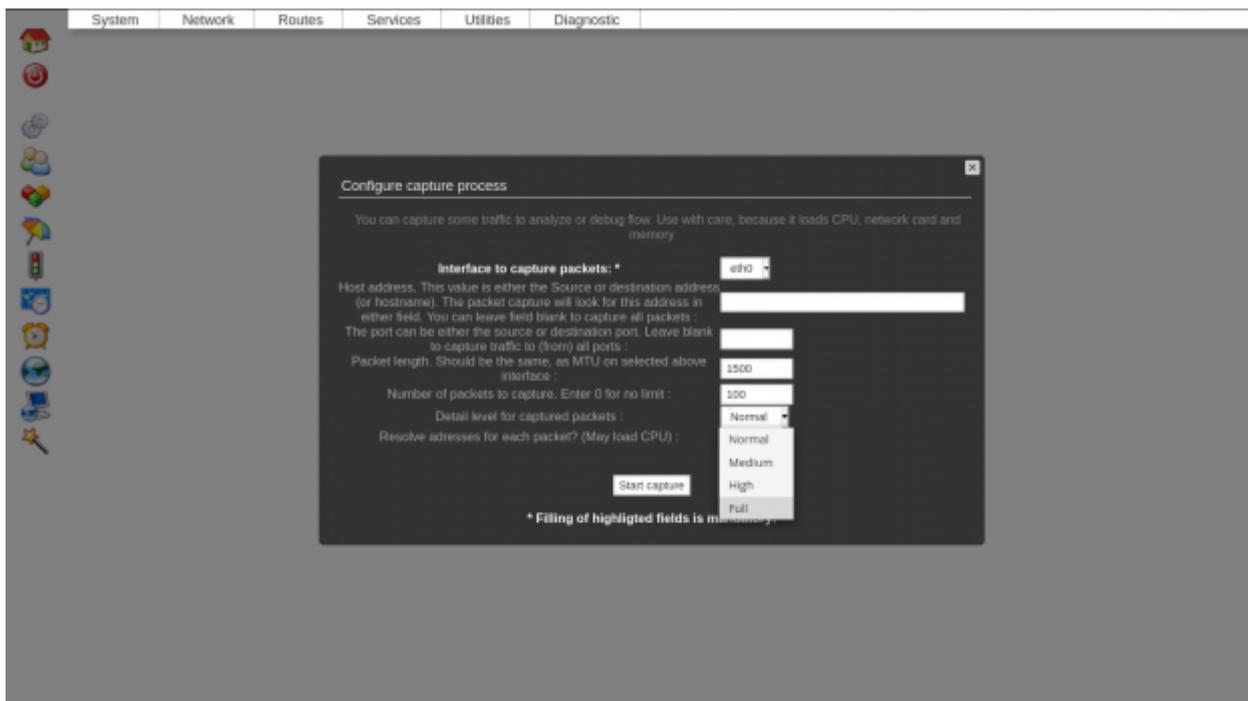


или «Утилиты→Захват пакетов» в русскоязычной.

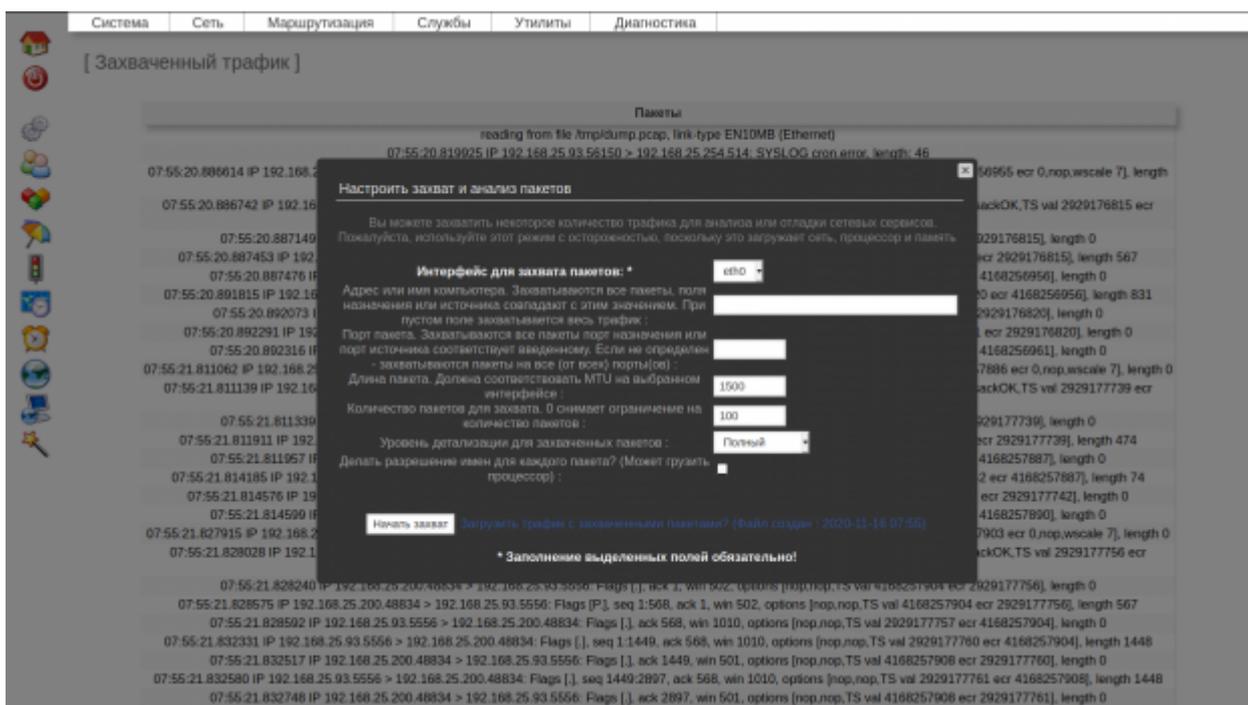


В появившемся диалоге присутствуют несколько полей для настройки захвата, которые мы рассмотрим ниже, кнопка «Начать захват», а также может присутствовать ссылка на загрузку файла, а под окном настроек присутствует перечень захваченных пакетов с краткой информацией о них (при условии, что со времени последней перезагрузки устройства

выполнялся захват пакетов).



Вариант отображения русскоязычного интерфейса при наличии файла захвата.



Рассмотрим назначение элементов / полей формы

Поле «Интерфейс для захвата пакетов» / «Interface to capture packets» по-умолчанию пустое. Для начала захвата необходимо из списка выбрать интерфейс, на котором будет производиться захват.

Необязательное к заполнению поле «Адрес или имя компьютера» / «Host address» по-умолчанию пустое. Если указать IP-адрес или имя, то будут захвачены только пакеты, адрес

отправителя или получателя которых соответствует указанному. Если указать имя, то необходимо также отметить «Делать разрешение имен» / «Resolve addresses for each packet». Пожалуйста, будьте **ОЧЕНЬ** аккуратны с использованием имен и последней опцией, поскольку она радикально замедляет захват пакетов.

Необязательное к заполнению поле «Порт пакета» / «The port...» по-умолчанию пустое. При указании значения, будут захватываться пакеты протоколов TCP и UDP, у которых порт равен данному значению.

Необязательное к заполнению поле «Длина пакета» / «Packet length» по-умолчанию пустое. При указании иного значения, будут захватываться все пакеты, размер которых точно соответствует указанному.

Необязательное к заполнению поле «Количество пакетов» / «Number of packets to capture» по-умолчанию равно 100. При указании иного значения отличного от нуля, будут захвачено указанное количество пакетов и процесс автоматически завершится. Процесс можно завершить командой досрочно. Пожалуйста, будьте **ОЧЕНЬ** аккуратны с большим или неограниченным количеством пакетов.

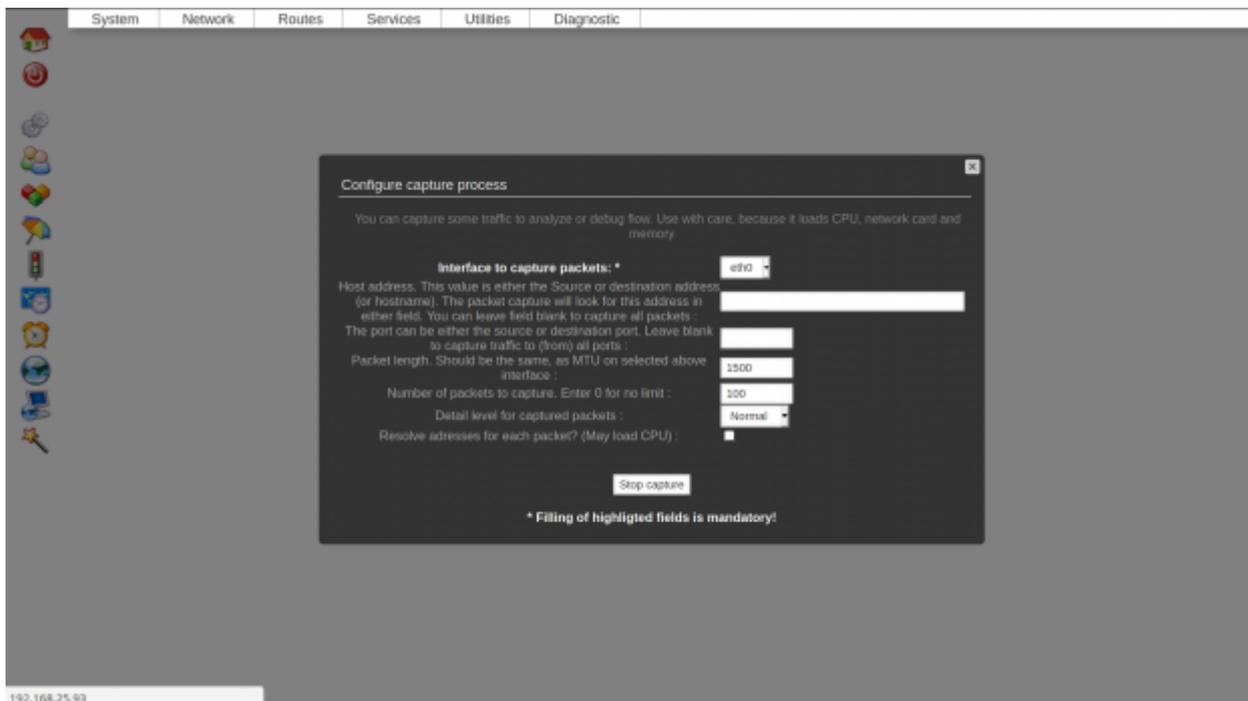
Необязательное к заполнению поле «Уровень детализации для захваченных пакетов» / «Detail level» по-умолчанию равно «Нормальный» / «Normal» (самый низкий уровень детализации). Имеет четыре градации до самого высокого. Оказывает влияние на детализацию вывода уже захваченного файла в форму. Не влияет на степень детализации самого файла захвата.

Поле «Делать разрешение имен» / «Resolve addresses for each packet». Если отмечено, то для каждого адреса отправителя и получателя будет произведена попытка найти соответствующее символьное имя. Следует обязательно отметить при указании имени компьютера во втором поле формы. Настоятельно рекомендуем не использовать без крайней необходимости.

Непустое содержимое полей комбинируется. Например, можно указать интерфейс, адрес и порт. В этом случае будут захватываться проходящие через интерфейс UDP и TCP пакеты с адресом отправителя и получателя равным указанному и порт для которых равен указанному.

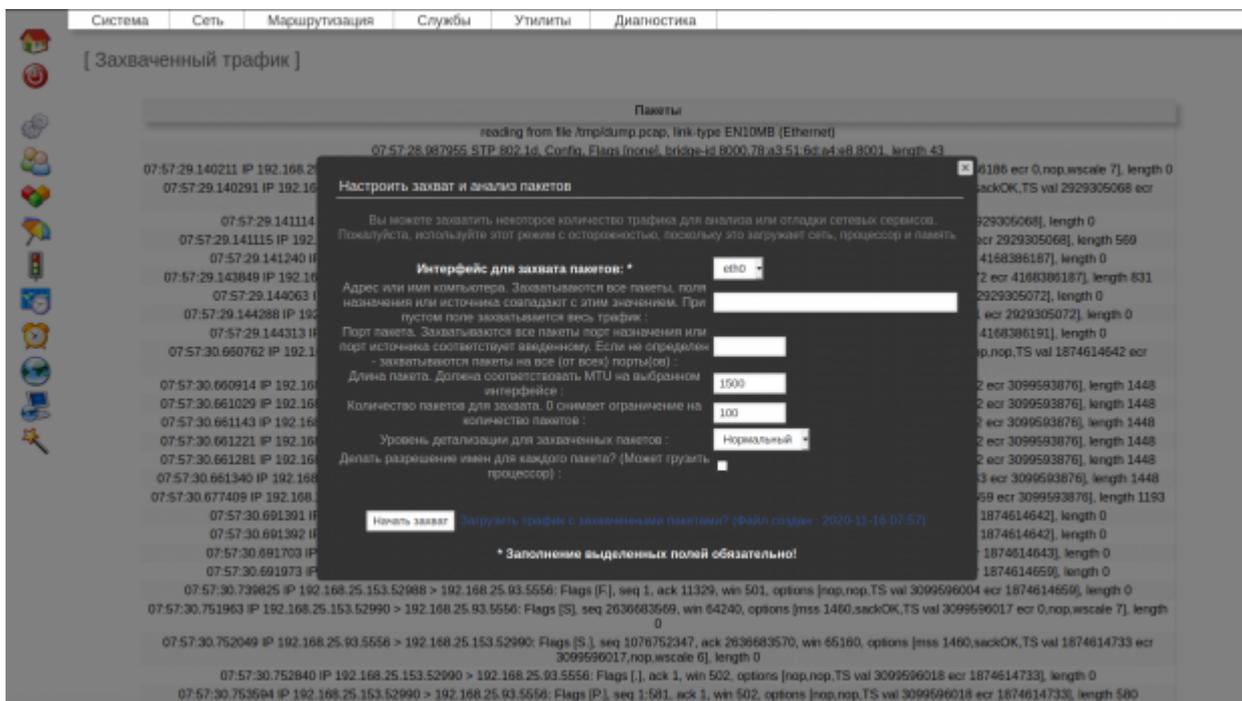
Кнопка «Начать захват» / «Start capture» начинает захват пакетов. Имеющийся файл захвата будет перезаписан. Присутствует на форме только когда нет активного процесса захвата.

Кнопка «Остановить захват» / «Stop capture» останавливает захват пакетов. Присутствует на форме только когда есть активный процесс захвата.



Ссылка для загрузки файла захвата на локальный компьютер и последующего анализа. Присутствует на форме только при наличии такого файла. Отображает время создания такого файла (по времени устройства).

Форма содержит элемент для своего закрытия (крестик в верхнем правом углу), что можно использовать для доступа к выводу результатов захвата.



Захват трафика из консоли

Для захвата трафика из консоли, необходимо подключиться к консоли устройства любым доступным способом:

- SSH
- Telnet
- Веб-консоль
- Физическая консоль

После получения доступа к консоли захват трафика следует делать командой `tcpdump`.

Пример команды для начала захвата трафика в консоли — `tcpdump -i eth0 -vvv -w /tmp/dump.pcap` (захватить весь трафик, проходящий через интерфейс eth0, показывать его с высокой степенью детализации и записывать в файл `dump.pcap` в каталоге `tmp`).

Остановить захват можно нажав `Ctrl+C`

Как удалить файл захвата без перезагрузки устройства?

Для удаления файла войдите в консоль устройства и дайте команду `rm -f /tmp/pcap.bin`

From: <http://docs.netshe-lab.ru/> - Документация по NETSHe

Permanent link: http://docs.netshe-lab.ru/doku.php?id=%D0%B7%D0%B0%D1%85%D0%B2%D0%B0%D1%82_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%BE%D0%B2_%D0%B2_netshe

Last update: 2020/11/16 06:35

