

Утилиты ping, traceroute, tcprdump

Спикер:

куплено на
Марат Сибгатулин - eucariot
SKLADCHIK.COM



СВЯТАЯ СЕТЕВАЯ ТРОИЦА

ping



tracertoute/tracepath/mtr



tcpdump



PING

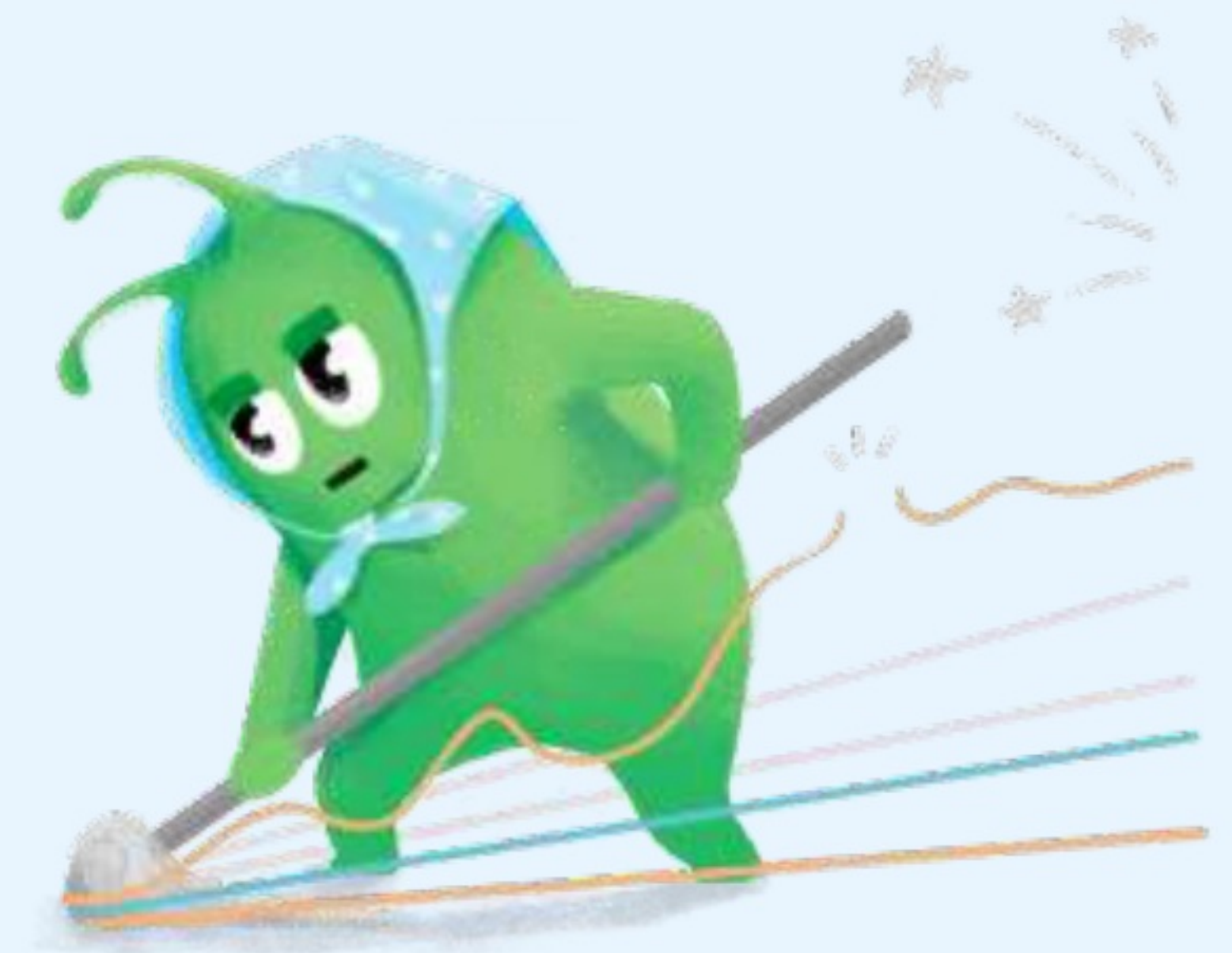
- Использует протоколы ICMP или ICMPv6
- Отправляет ICMP Echo Request, ожидает ICMP Echo Reply
- Замеряет RTT – Round Trip Time
- Иногда запрещён на фаерволах (в аду отдельный чанк для их админов)
- Работает напрямую поверх IP (без TCP и UDP)

Параметры:

- c** **N** – количество запросов (N штук)
- s** **M** – размер данных в запросе (M байтов)
- D** – для каждого запроса проставлять timestamp (Unixtime)
- I** **<intf>/<IP>** – указать интерфейс или IP-адрес, с которого нужно отправить запрос
- O** – явно показывать запросы без ответа
- i** **K** – интервал послыки запросов (K секунд)
- a** – пинг с бипом через динамик

TRACEROUTE/TRACERPATH

- Может использовать ICMP/TCP/UDP
- Отправляет серию запросов с увеличивающимся значением TTL и по сообщению ICMP Time Exceeded узнаёт каждый узел на пути
- В случае TCP/UDP шлёт данные на predetermined порт в диапазоне 33434-33534 или на указанный в команде
- Замеряет RTT
- Некоторые аргументы traceroute требуют права root. Tracerpath работает от рядового пользователя



MTR – МЛАДШИЙ И БОЛЕЕ КРАСИВЫЙ БРАТ TRACEROUTE

- Удобное отображение информации
- Постоянная, а не разовая отправка проверок
- Возможность выбирать протоколы и порты

Параметры:

-T – TCP

-u – UDP

-P – порт

-I – указать интерфейс, с которого будут отправляться запросы

-a – указать адрес, с которого будут отправляться запросы

TRACEROUTE, TRACEPATH, MTR



**Внимание! Attention! Achtung!
Attenzione!**



- Звёздочки и по reply ещё не означают, что есть проблемы
- Потери на промежуточных узлах ещё не означают, что есть проблемы
- Большие задержки на промежуточных узлах ещё не означают, что есть проблемы

Host	Packets		Pings				
	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. _gateway	0.0%	125	0.4	0.4	0.4	0.7	0.1
2. 10.200.5.178	0.0%	125	1.5	1.8	1.2	3.6	0.6
3. 10.200.16.128	0.0%	125	1.8	1.8	1.4	2.6	0.2
4. 10.200.16.192	0.0%	125	1.9	1.7	1.3	2.1	0.2
5. 10.200.16.53	0.0%	125	1.8	1.6	1.4	3.0	0.2
6. as6939.ix.dataix.eu	87.9%	125	21.8	25.5	21.8	53.1	8.4
7. 100ge0-35.core2.cph1.he.net	73.4%	125	30.1	31.0	29.5	45.9	3.9
8. ve951.core1.ewr5.he.net	0.0%	125	105.9	105.9	105.5	109.5	0.5
9. port-channel18.core3.ash1.he.net	61.3%	125	112.0	115.2	111.8	144.2	5.8
10. port-channel4.core3.lax2.he.net	82.3%	125	171.3	171.6	171.0	175.4	1.0
11. 100ge3-2.core1.lax2.he.net	0.0%	125	171.0	171.1	170.7	173.3	0.4
12. vocus.10gigabitethernet5-8.core1.lax2.he.net	9.6%	125	293.7	293.8	293.6	295.2	0.2
13. be101.bdr04.sjc01.ca.us.vocus.network	32.3%	125	306.9	307.0	306.8	308.2	0.2
14. be203.cor01.syd11.nsw.vocus.network	0.0%	125	312.1	311.9	311.7	312.5	0.2
15. (waiting for reply)							
16. (waiting for reply)							
17. (waiting for reply)							
18. be104.bdr02.bne03.qld.vocus.network	0.0%	125	309.8	310.1	309.5	324.8	1.5
19. 49.255.90.210	0.0%	124	310.1	310.2	310.0	310.7	0.1
20. nextdc-b2-pe1.bne.xi.com.au	0.0%	124	310.2	310.5	310.0	314.5	0.9
21. ip-103-95-114-117.bne.xi.com.au	0.0%	124	309.9	309.9	309.6	312.4	0.3

TCPDUMP

- Позволяет собирать и анализировать трафик, проходящий через узел
- Не только TCP – любой
- Требуется sudo

Параметры:

-i – выбрать интерфейс, на котором смотрим

-v/vv/vvv – более детализированный вывод

-host – фильтр по IP-адресу хостов (вариации: src, dst)

-port – фильтр по номеру порта

-ip/udp/tcp/icmp/icmp6/proto N – фильтр по протоколу

-and/or/not – операнды в фильтрах

-w – сохранить дампы в файл

TCPDUMP

```
ssh host 'sudo tcpdump -U -s0 not port 22 -w -' | /usr/local/bin/wireshark -k -i -
```



ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ

Где взять доступные адреса в разных странах?
<https://atlas.ripe.net/results/maps/network-coverage>

Все виды трассировок:
<https://hackware.ru/?p=9210>

tcpdump:
<https://hackware.ru/?p=10246>

Wireshark:
<https://linkmeup.ru/blog/753/>

