

Сетевые утилиты

В состав ИКС входят несколько сетевых утилит, которые помогают выполнять диагностику сети.

Пинг

ООО "Организация" > Сетевые утилиты

Администратор 115

Пинг

Трейс

Опрос Dns

Информация о домене

Дамп

Сетевые интерфейсы

Таблица маршрутизации

Тест скорости канала

Сканирование сети

Прокси access.log

Адрес *

Количество пакетов *

ya.ru

3

▶ Запустить

■

PING ya.ru (87.250.250.242): 56 data bytes

64 bytes from 87.250.250.242: icmp_seq=0 ttl=53 time=18.832 ms

64 bytes from 87.250.250.242: icmp_seq=1 ttl=53 time=23.266 ms

64 bytes from 87.250.250.242: icmp_seq=2 ttl=53 time=30.377 ms

ya.ru ping statistics ---

3 packets transmitted, 3 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 18.832/24.158/30.377/4.755 ms

Пинг (ping) — утилита для проверки соединений в сетях на основе TCP/IP. Она отправляет ICMP-запросы указанному узлу сети и фиксирует поступающие ответы. Время между отправкой запроса и получением ответа позволяет определять двусторонние задержки по маршруту и средний уровень потери пакетов, то есть определять стабильность и качество связи, а также косвенно определять загруженность на каналах передачи данных и промежуточных устройствах.

Также пингом называют время, затраченное на передачу пакета информации в компьютерных сетях от одного хоста до другого и обратно. Это время также называется лагом или задержкой и измеряется в миллисекундах. Задержка зависит от загруженности и количества узлов в пути между хостами.

ООО "Организация" > Сетевые утилиты

Пинг Трейс Опрос Dns Информация о домене Дамп Сет

Адрес *

Количество пакетов *

8.8.8.8

15

▶ Запустить

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=44 time=36.295 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=44 time=33.332 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=44 time=36.166 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=44 time=33.432 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=44 time=33.346 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=44 time=32.724 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=44 time=32.676 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=44 time=32.703 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=44 time=32.811 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=44 time=31.189 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=44 time=31.848 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=44 time=33.322 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=44 time=33.419 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=44 time=33.368 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=44 time=33.612 ms

--- 8.8.8.8 ping statistics ---
15 packets transmitted, 15 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 31.189/33.350/36.295/1.295 ms
```

Для запуска утилиты, необходимо ввести доменное имя или IP-адрес и указать количество пакетов.

Трейс

Трейс (tracert) - утилита для вывода маршрута прохождения запроса до выбранного хоста. Она выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к нему.

ООО "Организация" > Сетевые утилиты > Трейс

Пинг **Трейс** Опрос Dns Информация о домене Дамп Сетевые интерфейсы

Адрес * 8.8.8.8

▶ Запустить ☐

```
tracert to 8.8.8.8 (8.8.8.8), 64 hops max, 40 byte packets
 1  192.168.170.254 (192.168.170.254)  4.290 ms  5.065 ms  1.200 ms
 2  ysul-ccr1036-3.yar.ru (213.187.127.100)  1.373 ms  1.702 ms  1.228 ms
 3  ysul-asbr-0-vlan922.yar.ru (213.187.127.101)  1.186 ms  2.344 ms  1.526 ms
 4  178.176.156.73 (178.176.156.73)  13.166 ms  4.911 ms  2.586 ms
 5  dns.google (8.8.8.8)  31.005 ms  28.545 ms  29.612 ms
```

Эта утилита позволяет определить проблемы с маршрутизацией трафика, а также в случае проблем при доставке данных до какого-то узла - определить, на каком именно участке сети возникли неполадки.

Нужно отметить, что программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети. В силу особенностей работы протоколов маршрутизации в сети Интернет, обратные маршруты часто не совпадают с прямыми, причем это справедливо для всех промежуточных узлов в пути. Поэтому, ICMP-ответ от каждого промежуточного узла может идти своим собственным маршрутом, затеряться или прийти с большой задержкой, хотя в реальности с пакетами которые адресованы конечному узлу этого не происходит. Кроме того, на промежуточных маршрутизаторах часто стоит ограничение числа ответов ICMP в единицу времени, что приводит к появлению ложных потерь.

Опрос DNS

ООО "Организация" > Сетевые утилиты > Опрос Dns

Пинг

Трейс

Опрос Dns

Информация о домене

Дамп

Сетевые интерфейсы

Адрес *


Тип записи

DNS-сервер

ya.ru

A

(ИКС)

 Запустить

```
; <<>> DiG 9.14.7 <<>> ya.ru a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50747
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9ca3f4b8da1c7d99c3ac4ef75dbc20b08f27625612a2c09f (good)
;; QUESTION SECTION:
;ya.ru.                IN      A

;; ANSWER SECTION:
YA.ru.                 472     IN      A      87.250.250.242

;; AUTHORITY SECTION:
YA.ru.                 345472  IN      NS      ns2.yandex.RU.
YA.ru.                 345472  IN      NS      ns1.yandex.RU.

;; ADDITIONAL SECTION:
ns1.YANDEX.ru.         345472  IN      A      213.180.193.1
ns2.YANDEX.ru.         345472  IN      A      93.158.134.1
ns1.YANDEX.ru.         345472  IN      AAAA   2a02:6b8::1
ns2.YANDEX.ru.         345472  IN      AAAA   2a02:6b8:0:1::1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 01 15:10:24 MSK 2019
;; MSG SIZE rcvd: 229
```



Опрос DNS (dig) - позволяет посылать различные запросы к днс-серверам и определять ошибки в их конфигурации.

При использовании необходимо ввести домен и выбрать тип записи, также можно указать конкретный dns сервер для опроса. Более подробно о типах записи смотрите в руководстве по использованию модуля DNS.

Информация о домене

Пинг Трейс Опрос Dns **Информация о домене** Дамп Сетевые интерф

Адрес *

 Запустить 

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.tcinet.ru

domain:     RU

organisation: Coordination Center for TLD RU
address:    8 Marta street 1, bld 12
address:    Moscow 127083
address:    Russian Federation

contact:    administrative
name:       .RU domain Administrative group
organisation: Coordination Center for TLD RU
address:    8 Marta street 1, bld 12
address:    Moscow 127083
address:    Russian Federation
phone:      +7 495 730 29 71
fax-no:     +7 495 730 29 68
e-mail:     ru-adm@cctld.ru
```

Информация о домене (whois) - позволяет получить информацию о владельце домена или диапазона ip-адресов, а также сопутствующую информацию (дата регистрации, контактные данные, тип домена, регистратор и т.д.) из базы данных WHOIS.

Дамп

Дамп (tcpdump) - отображает заголовки пакетов, проходящих через выбранный сетевой интерфейс. Позволяет диагностировать проблемы связанные с настройкой межсетевого экрана, маршрутизацией и работой сетевых сервисов.

Интерфейс	Протокол	Порт
em0 (em0)	(любой)	(любой)
<input checked="" type="radio"/> Хост		
<input type="text" value="(любой)"/>		
<input type="radio"/> Источник	Назначение	
<input type="text" value="(любой)"/>	<input type="text" value="(любой)"/>	
<input checked="" type="checkbox"/> Сохранить результат в файл		
<input type="button" value="Показать файлы"/>		
<input type="button" value="▶ Запустить"/>		
<pre>17:11:37.693868 IP 192.168.17.23.44086 > 192.168.88.31.81: Flags [.], ack 199499, win 1441, options [nop,nop,TS val 117862874 ecr 33: 17:11:37.693916 IP 192.168.88.31.81 > 192.168.17.23.44086: Flags [.], seq 205739:206987, ack 1, win 130, options [nop,nop,TS val 331: 17:11:37.693982 IP 192.168.88.31.81 > 192.168.17.23.44086: Flags [.], seq 206987:208235, ack 1, win 130, options [nop,nop,TS val 331: 17:11:37.694040 IP 192.168.88.31.81 > 192.168.17.23.44086: Flags [.], seq 208235:209483, ack 1, win 130, options [nop,nop,TS val 331: 17:11:37.694096 IP 192.168.17.23.44086 > 192.168.88.31.81: Flags [.], ack 201995, win 1441, options [nop,nop,TS val 117862874 ecr 33: 17:11:37.694132 IP 192.168.88.31.81 > 192.168.17.23.44086: Flags [.], seq 209483:210731, ack 1, win 130, options [nop,nop,TS val 331: 17:11:37.694214 IP 192.168.88.31.81 > 192.168.17.23.44086: Flags [.], seq 210731:211979, ack 1, win 130, options [nop,nop,TS val 331: 17:11:37.711851 IP 192.168.17.23.44086 > 192.168.88.31.81: Flags [.], ack 205739, win 1441, options [nop,nop,TS val 117862878 ecr 33: 17:11:37.711926 IP 192.168.88.31.81 > 192.168.17.23.44086: Flags [.], seq 211979:213227, ack 1, win 130, options [nop,nop,TS val 331: 17:11:37.712042 IP 192.168.88.31.81 > 192.168.17.23.44086: Flags [.], seq 213227:214475, ack 1, win 130, options [nop,nop,TS val 331: 17:11:37.712126 IP 192.168.88.31.81 > 192.168.17.23.44086: Flags [.], seq 214475:215723, ack 1, win 130, options [nop,nop,TS val 331: 17:11:37.712173 IP 192.168.17.23.44086 > 192.168.88.31.81: Flags [.], ack 208235, win 1441, options [nop,nop,TS val 117862878 ecr 33: < ></pre>		

Для запуска утилиты необходимо выбрать сетевой интерфейс, на котором будет выполняться сбор данных.

Для фильтрации сообщений возможно выбрать: протокол; указать порт; выбрать направление сетевого трафика для указываемого IP-адреса, «Хост» или «Источник/Назначение»; установить флаг «Сохранить результат в файл» и просмотреть сохраненные файлы dump (нажать на кнопку «Показать файлы»).

При нажатии на кнопку «Показать файлы» будет открыто новое диалоговое окно, в котором возможно скачать/удалить файлы dump, имеющие расширение ***.pcap**. Данные файлы возможно открыть, например, программой *Wireshark*.

Удаление дампов файлов, возможно организовать по времени или по объему на вкладке **Система**. **Стоит обратить внимание**, если запустить сбор дампа в файл и оставить вкладку открытой на долгое время, то файл с дампом может занять все свободное место на жестком диске.

↑ Экспорт

Удалить

↺

Название	Объем	Создан
tcpdump_em0_1583847757.pcap	396982	10.03.2020 16:42
tcpdump_em0_1583849490.pcap	750878	10.03.2020 17:11
tcpdump_em1_1583847830.pcap	904	10.03.2020 16:43
tcpdump_em1_1583849450.pcap	3780	10.03.2020 17:10

Ок

Сетевые интерфейсы

Пинг Трейс Опрос Dns Информация о домене Дамп **Сетевые интерфейсы** Таблица маршрутизации Тес

▶ Запустить

```
vmx0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=60039b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TSO4, TSO6, RXCSUM_IPV6, TXCSUM_IPV6>
    ether 00:50:56:8e:40:c0
    hwaddr 00:50:56:8e:40:c0
    inet 192.168.17.134 netmask 0xffffffff broadcast 192.168.17.255
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
    media: Ethernet autoselect
    status: active
vmx1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=60039b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TSO4, TSO6, RXCSUM_IPV6, TXCSUM_IPV6>
    ether 00:50:56:8e:4d:28
    hwaddr 00:50:56:8e:4d:28
    inet 192.168.170.134 netmask 0xffffffff broadcast 192.168.170.255
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
    media: Ethernet autoselect
    status: active
vmx2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=60039b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TSO4, TSO6, RXCSUM_IPV6, TXCSUM_IPV6>
    ether 00:50:56:8e:95:f0
    hwaddr 00:50:56:8e:95:f0
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
    media: Ethernet autoselect
    status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=680003<RXCSUM, TXCSUM, LINKSTATE, RXCSUM_IPV6, TXCSUM_IPV6>
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x4
    inet 127.0.0.1 netmask 0xff000000
    nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
    groups: lo
enc0: flags=41<UP,RUNNING> metric 0 mtu 1536
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
    groups: enc
pflog0: flags=141<UP,RUNNING,PROMISC> metric 0 mtu 33160
    groups: pflog
lo1: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
    options=680000<LINKSTATE, RXCSUM_IPV6, TXCSUM_IPV6>
    inet 172.77.77.253 netmask 0xffffffff
    inet 172.77.77.1 netmask 0xffffffff
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
    groups: lo
```

Утилита «Сетевые интерфейсы» позволяет получить сведения о состоянии всех интерфейсов ИКС. Она выводит результат команды `ifconfig`, позволяя узнать, какие ip-адреса назначены каждому интерфейсу, какие виртуальные интерфейсы созданы, а также проверить наличие сигнала в подключенном кабеле.

Таблица маршрутизации

Пинг Трейс Опрос Dns Информация о домене Дамп Сетевые интерфейсы **Таблица маршрутизации**

▶ Запустить

Routing tables

Internet:

Destination	Gateway	Flags	Netif	Expire
default	192.168.170.254	UGS	vmx1	
127.0.0.1	link#4	UH	lo0	
172.77.77.1	link#7	UH	lo1	
172.77.77.253	link#7	UH	lo1	
192.168.17.0/24	link#1	U	vmx0	
192.168.17.134	link#1	UHS	lo0	
192.168.170.0/24	link#2	U	vmx1	
192.168.170.134	link#2	UHS	lo0	

Internet6:

Destination	Gateway	Flags	Netif	Expire
::/96	::1	UGRS	lo0	
::1	link#4	UH	lo0	
::ffff:0.0.0.0/96	::1	UGRS	lo0	
fe80::/10	::1	UGRS	lo0	
fe80::%lo0/64	link#4	U	lo0	
fe80::1%lo0	link#4	UHS	lo0	
ff02::/16	::1	UGRS	lo0	

Данная утилита выводит текущую таблицу маршрутизации ИКС. С ее помощью вы можете увидеть все маршруты, созданные в системе.

Тест скорости канала

Эта утилита позволяет измерить пропускную способность канала. Для измерения необходимо выбрать сервер и запустить тест. Внимание! Не все сервера могут быть доступны. Также не все сервера могут показать подлинную скорость вашего канала из-за удаленности, количества промежуточных узлов и их загруженность.

Сканирование сети

Пинг

Трейс

Опрос Dns

Информация о домене

Дамп

Сетевые интерфейсы

Таблица маршрутизации

Тест скорости канала

Сканирование сети

Действие

Адрес

Порт

Сканирование портов

192.168.17.134

▶ Запустить

Starting Nmap 7.70 (https://nmap.org) at 2019-11-01 15:15 MSK
Initiating System DNS resolution of 1 host. at 15:15
Completed System DNS resolution of 1 host. at 15:15, 0.03s elapsed
Initiating SYN Stealth Scan at 15:15
Scanning 192.168.17.134 [100 ports]
Discovered open port 22/tcp on 192.168.17.134
Discovered open port 53/tcp on 192.168.17.134
Discovered open port 3128/tcp on 192.168.17.134
Discovered open port 81/tcp on 192.168.17.134
Increasing send delay for 192.168.17.134 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
Discovered open port 389/tcp on 192.168.17.134
Completed SYN Stealth Scan at 15:15, 14.73s elapsed (100 total ports)
Nmap scan report for 192.168.17.134
Host is up (0.000045s latency).
Not shown: 95 filtered ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
81/tcp open hosts2-ns
389/tcp open ldap
3128/tcp open squid-http

Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.88 seconds
Raw packets sent: 495 (21.780KB) | Rcvd: 555 (24.420KB)

С помощью сканирования сети вы можете тестировать безопасность локальной сети предприятия. Она позволяет проверить доступность локальных машин, а также определить открытые в сети порты. Кроме того, указав в качестве исследуемого хоста сам ИКС, вы можете дополнительно проверить безопасность системы на предмет доступных портов.

Сканирование сети может работать в трех режимах:

Режим	Действия
Доступность адресов	ИКС проверяет, в сети ли выбранные машины. В качестве аргумента может быть указан как отдельный хост, так и подсеть. В последнем случае ИКС проверит доступность всего указанного диапазона перебором.
Сканирование портов	ИКС проверяет, какие порты открыты для доступа на указанном хосте или всех машинах указанной подсети
Информация о версии	ИКС проверяет версию службы каждого открытого порта на указанном хосте или всех машинах указанной подсети

From:
<https://doc-old.a-real.ru/> - **Документация**

Permanent link:
<https://doc-old.a-real.ru/doku.php?id=ics70:netutil>

Last update: **2020/03/11 14:02**

