

Про пинги



- Мыкола, ты слышал, як москали ICMP-пакеты называють? - Як? - Пинги!

Пинги это такие запросы типа Echo-Request протокола Internet Control Message Protocol (ICMP) указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT, от англ.Round Trip Time) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определять загруженности каналов передачи данных и промежуточных устройств. Также пингом называется время, затраченное на передачу пакета информации в компьютерных сетях от клиента к серверу и обратно от сервера к клиенту, оно измеряется в миллисекундах. Время пинга связано со скоростью соединения и загруженностью каналов на всём протяжении от клиента к серверу. Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.

Программа ping является одним из основных диагностических средств в сетях TCP/IP и входит в поставку всех современных сетевых операционных систем. Функциональность ping также реализована в некоторых встроенных ОС маршрутизаторов.

Всегда

Всегда пасуем и стейтим следующие типы. 0,3,4,8,11

```
icmp_serve = "0,3,4,8,11"
pass in on $ttk reply-to ($ttk $ttk_gw) inet proto icmp icmp-type {
    $icmp_serve } keep state
pass in on $ttk inet proto icmp from ($ttk:network) icmp-type { $icmp_serve
} keep state
```

Типы ICMP

1. 0 echo-reply
2. 3 destination unreachable
 1. 1 = host unreachable
 2. 2 = protocol unreachable
 3. 3 = port unreachable
 4. 4 = fragmentation needed and DF set
 5. 5 = source route failed
 6. 4 source-quench
4. 5 redirect
 1. code 0 = redirect datagrams for the network
 2. 1 = redirect datagrams for the host
 3. 2 = redirect datagrams for the type of service and network

4. 3 = redirect datagrams for the type of service and host
5. 6 alternate-address
6. 8 echo request
7. 9 router-advertisement
8. 10 router-solicitation
9. 11 time-exceeded
 1. 0 = time to live exceeded in transit
 2. 1 = fragment reassembly time exceeded
10. 12 parameter-problem
11. 13 timestamp-request
12. 14 timestamp-reply
13. 15 information-request
14. 16 information-reply
15. 17 mask-request
16. 18 mask-reply
17. 31 conversion-error
18. 32 mobile-redirect

ПИНГИ И ЦИСКИ

Многие знают и умеют пользоваться командой ping и traceroute, но не все знают, что же означают символы выводимые на консоль в устройствах Cisco Systems:

```
Router1#debug ip packet detail
IP packet debugging is on (detailed)

Router1#ping 12.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.0.0.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

Router1#
Jan 20 15:54:47.487: IP: s=12.0.0.1 (local), d=12.0.0.2 (Serial0), len 100,
sending
Jan 20 15:54:47.491: ICMP type=8, code=0

!--- Это ICMP пакет от 12.0.0.1 для 12.0.0.2.
!--- ICMP type=8 это echo request (запрос).

Jan 20 15:54:47.523: IP: s=12.0.0.2 (Serial0), d=12.0.0.1 (Serial0), len
100, rcvd 3
Jan 20 15:54:47.527: ICMP type=0, code=0

!--- А это ответ от 12.0.0.2.
!--- ICMP type=0 это echo reply (ответ).
```

Рассмотрим символы выводимые в консоль cisco при команде ping:

```
! - Каждый символ восклицательно знака показывает ответ (echo reply).
. - Каждый символ точки показывает потерю пакета, таймаут ожидания (echo reply).
U - Указанный хост недостижим (был получен destination unreachable error PDU).
Q - сдерживание источника (есть угроза перегрузки (destination too busy)).
M - Невозможность фрагментировать.
? - Неизвестный тип пакета.
& - Время жизни пакета истекло.
```

трейсы и циски

tracert — это служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Tracert так же как и ping основана на протоколе ICMP.

Программа tracert выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки.

tracert входит в поставку большинства современных сетевых операционных систем:

1. в системах Microsoft Windows эта программа носит название tracert
2. в системах Unix — tracert

Для определения промежуточных маршрутизаторов tracert отправляет серию пакетов данных целевому узлу, при этом каждый раз увеличивая на 1 значение поля TTL («время жизни»). Это поле обычно указывает максимальное количество маршрутизаторов, которое может быть пройдено пакетом. Первый пакет отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно сообщение ICMP, указывающее на невозможность доставки данных. Tracert фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа (эти сведения выводятся на монитор компьютера). Затем tracert повторяет отправку пакета, но уже с TTL, равным 2, что позволяет первому маршрутизатору пропустить пакет дальше.

Процесс повторяется до тех пор, пока при определённом значении TTL пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым.

Пример команды на оборудовании Cisco Systems:

```
Router1#tracert 34.0.0.4

Type escape sequence to abort.
Tracing the route to 34.0.0.4

 1 12.0.0.2  4 msec  4 msec  4 msec
 2 23.0.0.3 20 msec 16 msec 16 msec
 3 34.0.0.4 16 msec * 16 msec
```

В консоль так же могут выводиться спец. символы, вот они:

- * – Таймаут ожидания ответа (`timed out`)
- A – Административно запрещено (трафик запрещен администратором сети, например в `access-list`)
- Q – сдерживание источника (есть угроза перегрузки (`destination too busy`)).
- I – Пользователь прервал выполнение теста
- U – Порт недостижим (закрыт)
- H – Хост недоступен (`unreachable`), например отсутствует маршрут до сети хоста
- N – Сеть недоступна (`unreachable`)
- P – Протокол недоступен (`unreachable`)
- T – Таймаут (`timeout`)
- ? – Неизвестный тип пакета

From:
<https://wiki.rtzra.ru/> - RTzRa's hive

Permanent link:
<https://wiki.rtzra.ru/internet/ping>

Last update: **2017/05/09 18:34**

