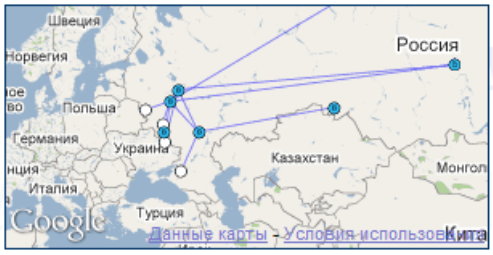
О чем расскажет traceroute

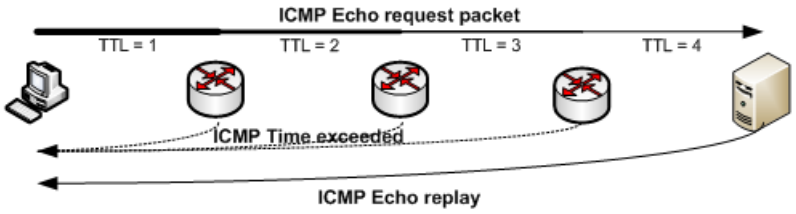


В инструментарий первичной диагностики неполадок в сетях на базе стека протоколов TCP/IP, утилита traceroute вошла уже давно. Общая идея алгоритма осталась неизменной еще с 1987 года, когда она впервые была реализована программно Van Jacobson, сотрудником группы сетевых исследований (Network) в Национальной лаборатории Беркли (Lawrence). За более чем 20-ти летний период времени, этот простой в использовании инструмент стал обыденным и привычным, и мало уже кто задумывается о том, что получаемые результаты «трассировки» хорошо демонстрируют один из краеугольных принципов построения сетей связи. Речь идет об аспекте **разграничения зон обслуживания**, на котором в том числе тоже держится связь, и о котором сейчас часто забывают.

Он хорошо известен связистам «старой школы», когда требование работоспособности в пять девяток считалось не нонсенсом, как сейчас, а всего лишь заурядным показателем работы систем телефонной связи. Дома могло не быть света, - где-то оборвало электрический кабель, висящий на опорах. Воду могли отключить, - на водонапорной башне отключили электроэнергию, потому что «где-то оборвало кабель, висящий на опорах»... Вот только телефон, правда, у тех у кого он имелся в наличии, должен был работать. И даже сейчас, имея дома уже много лет обыкновенный кнопочный аппарат, я так и не смог вспомнить, когда последний раз обращался к своему оператору телефонной связи с какой-то жалобой на аварию. Понятно, я утрирую. Но все-таки, а Вы вспомните?

Совершенно другая ситуация наблюдается в сетях «нового» мира, мира пакетной передачи, ярким проявлением которого является уже такое обыденное явление как интернет. Ирония в том, что сам интернет, в своей первоначальной ипостаси вышел из проекта ARPANET, - как ответ министерства обороны США для надежной системы передачи информации на случай глобальной ядерной войны и тотальных разрушений. Так почему же сейчас, когда призрак ядерной войны ушел в небытие, а катаклизмы и разрушения в своей массе затрагивают нас очень редко - ситуация кардинально иная? Стоит взглянуть на ветку форума «XYZ» этого сайта. Топик существует чуть более года, а счетчик сообщений скоро перешагнет полторы тысячи. И это только по магистральным каналам связи, аварии на которых затрагивают значительные группы абонентов. В чем дело?

Прежде чем ответить на вопрос, надо вернуться к теме статьи, вынесенной в ее заголовок, утилите traceroute. Как оказалось, на сайте бывают и обыкновенные пользователи, хоть и продвинутые. Небольшой ликбез не помешает. Суть алгоритма утилиты очень проста: в IP-пакетах поле TTL (Time To Live) задает время жизни отправленной в сеть дейтаграммы. Каждый узел, который обрабатывает пакет и пересылает его дальше, уменьшает значение поля TTL на единицу. Когда TTL становится равным 1 или 0, пакет уничтожается, а отправителю отсылается сообщение ICMP «time exceeded» (время превышено). Нужно это для того, что бы дейтаграмма бесконечно не «гуляла» по сети, если не сможет дойти до адресата. Максимальное значение TTL ограниченно его разрядностью (8 бит) и составляет 255, реальные же значения устанавливаются каждой системой по разному. Стоит отметить, что TTL также уменьшается каждую секунду нахождения его на узле, хотя для современных сетей это часто не принципиально, за исключением, наверное, «шейпера» трафика (bandwidth control, ограничение полосы) с достаточно жесткими параметрами.



Пример реализации traceroute

Именно механизм TTL задействован для определения пути следования пакета. Классическая реализация traceroute посылает серию из трех UDP-пакетов на произвольный порт (по умолчанию 33434) с TTL = 1. По поступлению ответов ICMP «time exceeded» определяется время прохождения и доменное имя узла. Затем процедура повторяется с TTL = TTL + 1 до тех пор, пока пакет не достигнет конечного узла, который ответит «port unreachable» (порт не доступен). В зависимости от реализации, вариации traceroute могут различаться. К примеру, консольная утилита tracert.exe в

семействе Windows использует запросы ICMP «echo», которые обычно используются утилитой ping. В любом случае, результат работы утилиты будет включать в себя определенный набор информации: список узлов, через которые проходит пакет от адреса источника до адреса назначения и задержки при передаче пакетов. Последний важный аспект. Нельзя забывать, что пути пакетов в интернет неисповедимы. Уходя одним путем, ответ на запрос может возвращаться другим. Поэтому для анализа полной информации нужны результаты traceroute и с обратной стороны.

Hop	Host	C	Loss%	ASN	best	Avg	worst	Country	BGP Prefix	ASName
3	D 99-185-40-2.lightspeed.sntcca.sbcglobal.	4	20%	7132	437.9	595.97	844.2	US	99.176.0.0/12	SBIS-AS - AT&T Inte
4	D 71.145.12.202	1	80%	7132	21.9	21.9	21.9	US	71.128.0.0/11	SBIS-AS - AT&T Inte
6	D 71.145.0.4	1	80%	7132	22.7	22.7	22.7	US	71.128.0.0/11	SBIS-AS - AT&T Inte
7	D 151.164.55.0	5	0%	7132	20.9	21.06	21.2	US	151.164.0.0/16	SBIS-AS - AT&T Inte
8	D 12.122.137.217	5	0%	7018	21.7	21.94	22.2	US	12.0.0.0/9	ATT-INTERNET4 - AT&
9	D 192.205.34.34	5	0%	7018	23.4	39.36	102.5	US	192.205.32.0/22	ATT-INTERNET4 - AT&
10	D te2-4.mpd01.sjc03.atlas.cogentco.com	5	0%	174	23.2	23.64	24	US	154.48.0.0/12	COGENT Cogent/PSI
11	D te3-2.mpd01.sjc01.atlas.cogentco.com	5	0%	174	24.1	26.46	35	US	154.48.0.0/12	COGENT Cogent/PSI
12	D te0-0-0-4.mpd21.sfo01.atlas.cogentco.com	5	0%	174	24.9	25.18	25.5	US	154.48.0.0/12	COGENT Cogent/PSI
13	D te0-0-0-2.mpd21.mci01.atlas.cogentco.com	5	0%	174	68.5	68.68	68.9	US	154.48.0.0/12	COGENT Cogent/PSI
14	D te0-2-0-3.mpd21.ord01.atlas.cogentco.com	5	0%	174	73.7	73.92	74.1	US	154.48.0.0/12	COGENT Cogent/PSI
15	D te0-3-0-4.mpd21.dca01.atlas.cogentco.com	5	0%	174	94.4	94.72	95	US	154.48.0.0/12	COGENT Cogent/PSI
16	D te0-3-0-6.mpd21.fra03.atlas.cogentco.com	5	0%	174	193.6	194.3	194.7	US	154.48.0.0/12	COGENT Cogent/PSI
17	D te3-3.ccr01.fra06.atlas.cogentco.com	4	20%	174	193.6	220.48	299.3	US	130.117.0.0/16	COGENT Cogent/PSI
18	D 149.6.42.6	5	0%	174	242.5	242.66	242.8	US	149.6.0.0/16	COGENT Cogent/PSI
19	D 85.112.112.18	4	20%	25478	243.5	250.02	268.3	RU	85.112.112.0/20	IHOME-AS iHome Auto
20	D ihome.nag.ru	4	20%	25478	244.3	244.58	245	RU	85.112.112.0/20	IHOME-AS iHome Auto

Пример результата работы traceroute. http

Так вот, возвращаясь к поставленному ранее вопросу «в чем дело?» теперь можно и ответить. То есть указать всего лишь один из возможных вариантов ответа. Наверное, во всем виноваты программисты. Как говорит известная притча, «если бы они строили цивилизацию, то залетевшая внутрь птица развалила бы ее как карточный домик». Именно программисты внесли в связь, лет пятнадцать с лишком назад еще девственную и непорочную, свою культуру, взятую от утверждения, где «**баг и не баг вообще, а просто фича**». Да, да, - это шутка! И все-таки доля правды в ней есть. Телеком, стоя на острие инновационного развития, порожденного информационно-компьютерными технологиями, сам же и развивался за счет них. Хотите пример взаимной интеграции? Пожалуйста. Попробуйте навскидку определить, что делает нижеприведенный код:

int f1 (int a, int b) { if (sign(a) != sign(b)) return (a+b)/2; else return a+(b-a)/2; }

Угадали? А ведь все очень просто. Это функция для вычисления среднего значения двух аргументов. А теперь определите по приведенному ниже скану из форума, где находятся зоны ответственности операторов с точки зрения простого пользователя, грешным делом решившего запустить стандартную для Windows (>90% абонентов) версию tracert, чтобы попробовать понять, на чьей стороне проблема. Только, пожалуйста, без всяких там whois сервисов, о которых даже продвинутый пользователь имеет право не знать.

```
1 <1 мс <1 мс <1 мс 192.168.1.1
2 16 ms 17 ms 12 ms 85.175.1.67
3 10 ms 10 ms 11 ms 85.175.1.101
4 11 ms 10 ms 29 ms 85.175.1.119
5 11 ms 10 ms 11 ms 85.173.2.4
6 11 ms 10 ms 10 ms 85.173.1.244
7 11 ms 10 ms 11 ms 87.226.233.173
8 29 ms 29 ms 29 ms ae-8.m7-ar4.msk.ip.rostelecom.ru [87.226.133.178
9 106 ms 106 ms 106 ms xe231-201.RT.M9.MSK.RU.retn.net [87.245.255.37]
10 118 ms 118 ms 127 ms ae0-9.RT.BOR.SPB.RU.retn.net [87.245.233.10]
11 159 ms 130 ms 130 ms GW-InfoBox.retn.net [87.245.250.98]
12 118 ms 118 ms 118 ms 77.221.142.90.addr.datapoint.ru [77.221.142.90]
```

```
1 ae0-5.RT.MR.MSK.RU.retn.net (87.245.233.122) 12.483 ms 12.426 ms ae1-9.RT.MR.MSK.RU.r
2 GW-Synterra.retn.net (87.245.253.170) 12.863 ms 12.807 ms 63.371 ms
3 msk-d2-hq-ae2.main.synterra.ru (83.229.225.9) [AS 6854] 12.456 ms 12.444 ms 12.084 ms
4 GW-Megafon.main.synterra.ru (83.229.193.22) [AS 6854] 43.004 ms 41.298 ms 62.830 ms
5 85.26.172.214 (85.26.172.214) [AS 31133] 86.048 ms 45.637 ms 73.935 ms
6 85.173.1.245 (85.173.1.245) [AS 44467] 90.764 ms 35.109 ms 34.295 ms
7 85.173.2.5 (85.173.2.5) [AS 44467] 174.594 ms 248.384 ms 173.038 ms
8 85.175.1.116 (85.175.1.116) [AS 25490] 179.808 ms 168.299 ms 135.760 ms
9 85.175.1.67 (85.175.1.67) [AS 25490] 160.865 ms 97.383 ms 136.899 ms
```

Скан сообщений (от 16.02.2010) из топика «XYZ упал:(» с форума NAG.ru

Не правда ли, очень гармонирует с примером функции вычисления среднего значения? И там и там страдает визуализация. В первом случае визуализация программного кода осложнена записью в одну строку. Во втором случае отсутствие имен узлов мешает пользователю отследить пути следования пакетов. Отметим, что эта беда не только российских компаний. Она международного характера. В приведенном выше примере traceroute через webtrace.info надо смотреть на AS7132 и AS7018. А ведь если проблема действительно находится за пределами сети оператора, здравые имена узлов позволяют снизить поток жалоб от абонентов в адрес оператора. Ведь оперировать к именам, имеющим значение, всегда проще, чем к каким-то там цифрам. Ясно, что таких клиентов, пытливый ум которых будет стремиться узнать, из-за кого провайдера «та сволочь в любимой онлайн - игре отстрелила ему башку», - очень мало. Насколько активны они в форумах, мне судить сложно.

Только есть еще и другая группа потребителей. Я говорю о корпоративных пользователях, тех, у кого есть или системные администраторы, или даже целые отделы ИТ. Корректно ли заставлять их «лезть» в ripe, чтобы определить стыки, а значит и зоны ответственности сетей, когда интернет не работает или «работает, но как-то не так»?! В ответ появляются такие решения, как «Улучшитель

кармы трафика». Для тех, кто побогаче - аппаратное решение, а для тех, кто победней скоро планируется выпуск программного продукта. А если серьезно? Может ли видимое пренебрежение оператора к разграничению зон ответственности являться пренебрежением реальным? Вероятно, нет. Зная уровень технических специалистов ЮТК, попавшей в примеры к статье, - НЕТ с уверенностью в 99,999%. Знает ли об этом клиент?! Вероятно, ТОЖЕ нет. Поэтому в случае аварии **tracert** свою функцию выполнит и **расскажет** клиентам, и так изнывающим, о том, что якобы их **провайдер не может** даже имя узлов «сконфигурировать». О каком уж там разделении зон ответственности вести речь? Стоит ли этого мнения призрачная безопасность топологии сети, а может и просто нежелание немного «повозиться»? Пускай каждый провайдер решает для себя сам...

Дополнительные материалы: A Practical Guide to (Correctly) Traceroute with Troubleshooting.