Принцип действия утилиты traceroute

целевому узлу отправляется серия icmp пакетов в качестве адреса назначения всегда указывается целевой узел

Первая серия пакетов отправляется с TTL=1

первый маршрутизатор возвращает icmp сообщение <time exceeded in transit>

traceroute фиксирует: адрес маршрутизатора, время между отправкой пакета и получением пакета

Вторая серия пакетов отправляется с TTL=2

первый маршрутизатор уменьшает TTL на 1 и направляет пакеты по второму маршрутизатору.Второй маршрутизатор получив пакеты с TTL = 1 , также возвращает <time exceeded in transit>

traceroute фиксирует: адрес маршрутизатора, время между отправкой пакета и получением пакета

Третья серия пакетов отправляется с TTL=3

первый маршрутизатор уменьшает TTL на 1 и направляет пакеты по третьему маршрутизатору.Третий маршрутизатор получив пакеты с TTL = 2 , также возвращает <time exceeded in transit>

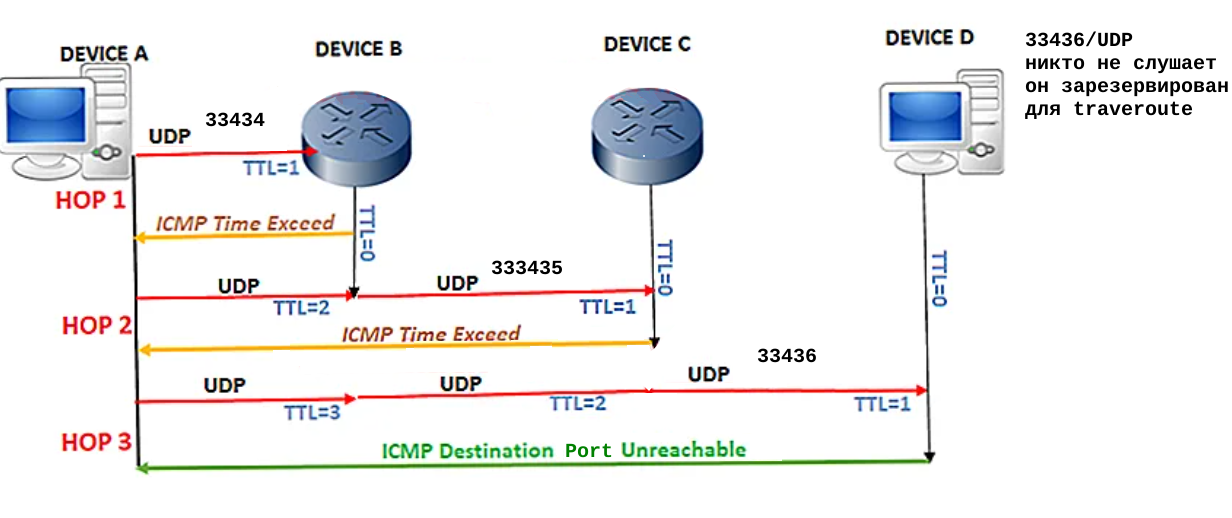
traceroute фиксирует: адрес маршрутизатора, время между отправкой пакета и получением пакета

Ит.д значение с каждым шагом поля TTL увеличивается на 1.

Если это искомый узел, то приходит REPLY если это ICMP или UDP порт недостижим, если UDP.

Если рассмотреть на графическом примере:

то,



Есть 2 хоста,между ними 2 маршрутизатора.

1)Запускаем утилиту traceroute с хоста 1 на хост 2 т.к TTL = 1, то происходит обрыв связи на DEVICE B

2)Запускаем утилиту traceroute с TTL = 2, с хоста 1 на хост 2, т.к здесь TTL = 2 то происходит обрыв связи на DEVICE С

3)Запускаем утилиту traceroute с TTL = 3, с хоста 1 на хост 2 утилита видит что ответ приходит от узла от которого была запущена утилита traceroute в ответ идет ответ ICMP что порт недостижим.(это и означает что узла мы как раз достигли.)