Использование команды traceroute в операционных системах

Содержание

Введение

Команда traceroute позволяет определить путь, которым пакет проходит к месту назначения из данного источника, путем возвращения отправителю информации о последовательности переходов пакета из одной сети в другую. Эта служебная программа входит в комплект операционной системы хоста (например, Linux или Microsoft (MS) Windows), а также ПО Cisco IOS®.

Предварительные условия

Требования

У читателей данной документации должны быть базовые знания об одной из этих операционных систем:

- ПО Cisco IOS)
- Linux
- Microsoft Windows

Используемые компоненты

Сведения в этом документе применяются к этим версиям программного и аппаратного обеспечения:

- Маршрутизатор Cisco, который выполняет программное обеспечение Cisco IOS версии 12.2 (27)
- ПК, который выполняет Версию Red Hat Linux 9
- ПК, который выполняет MS Windows 2000

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Общие принципы работы

При выполнении *команды ip address* **traceroute** на исходном устройстве (таком как хост или маршрутизатор, действующий как хост), она передает пакеты IP к назначению со значениями Времени жизни (TTL), которые инкрементно увеличиваются до максимального указанного счетчика переходов. Это равняется 30 по умолчанию. Как правило, каждый маршрутизатор в пути к назначению постепенно уменьшает поле TTL одним модулем, в то время как это передает эти пакеты. Когда маршрутизатор посреди пути находит пакет с TTL = 1, это отвечает сообщением "time exceeded"(превышение времени) Протокола ICMP к источнику. Это сообщение позволяет источнику знать, что пакет пересекает тот конкретный маршрутизатор как переход

Существуют некоторые различия для способа**, которым команда traceroute** внедрена в различном этом документе операционных систем, обсуждает.

Cisco IOS и Linux

TTL для Протокола передачи дэйтаграмм исходного пользователя (UDP) тестовая дэйтаграмма установлен в 1 (или минимальный TTL, как задано пользователем в команде расширенной трассировки. Целевой порт UDP зонда исходной датаграммы установлен в 33434 (или, как задано в выходных данных **команды расширенной трассировки**). **Команда расширенной трассировки** является изменением обычной **команды traceroute**, которая позволяет значениям по умолчанию параметров, используемых операцией **traceroute**, таких как TTL и номер порта назначения модифицироваться. Для получения дополнительной информации о том, как использовать **команду расширенной трассировки**, обратитесь к Использованию Команды extended ping и Команд расширенной трассировки. Исходный порт UDP зонда исходной датаграммы рандомизирован и имеет логического оператора OR с 0x8000 (гарантирует минимальный исходный порт 0x8000). Эти шаги иллюстрируют то, что происходит, когда запущена дейтаграмма UDP:

Примечание: Параметры конфигурируемы. Данный пример запускается с n = 1 и

заканчивается с n = 3.

1. Дейтаграмма UDP диспетчеризирована с TTL = 1, целевой порт UDP = 33434, и рандомизированный исходный порт.
2. Порт получателя UDP инкрементно увеличен, исходный порт UDP рандомизирован, и вторая диспетчеризированная дейтаграмма.
3. Шаг 2 повторен максимум для трех зондов (или как много раз согласно просьбе в выходных данных **команды расширенной трассировки**). Для каждого из передаваемых зондов вы получаете "TTL, превышенный" сообщение, которое используется для построения пошагового пути к адресату.
4. Если сообщение "time exceeded"(превышение времени) ICMP получено, TTL инкрементно увеличен, и этот цикл повторения с инкрементными номерами порта назначения. Можно также получить одно из этих сообщений:Тип ICMP 3, код 3 ("недостижимое назначение", "порт, недостижимый") сообщение, которое указывает, что был достигнут хост."Недостижимый узел", "недостижимая сеть", "максимальный TTL превысил", или тип сообщения "таймаута", что означает, что повторно передан зонд.

Маршрутизаторы Cisco передают тестовые пакеты UDP с портом исходного исходного и инкрементным портом назначения (для различения других зондов). Маршрутизаторы Cisco передают сообщение ICMP "время, превышенное" назад к источнику от того, где был получен пакет UDP/ICMP.

Команда traceroute Linux подобна внедрению маршрутизатора Cisco. Однако это использует неподвижный исходный порт.*-n* опция в **команде traceroute** используется для предотвращения запроса к серверу имен.

Microsoft Windows

Команда tracert MS Windows использует Датаграммы эхо-запроса ICMP вместо дейтаграмм UDP как зонды. Эхо-запросы протокола ICMP запущены с инкрементно увеличивающимся TTL, и та же операция, как описано в Cisco IOS и Linux происходит. Значение использования Датаграмм эхо-запроса ICMP состоит в том, что завершающий переход не полагается на ответ сообщения "unreachable" (недостижимый) ICMP от адресата. Это полагается вместо этого на Сообщение с эхо-ответом ICMP.

Синтаксис команды:

```
tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name
```

Эта таблица объясняет параметры командной строки:

Параметр	Описание
- d	Задает для не решения адресов к именам компьютера.
- h maximum_hops	Задает максимальное число переходов для поиска цели.
- j компьютерный список	Задает свободный исходный маршрут вдоль компьютерного списка.
- w таймаут	Ждет количество миллисекунд,

	заданных таймаутом для каждого ответа.
target_name	Название целевого компьютера.

Ограничение частоты сообщений ICMP о недостижимых адресах

Недостижимый ICMP ограничен одним пакетом на 500 мс (как защита для атак Отказа в обслуживании (DoS)) в маршрутизаторе Cisco. От программного обеспечения Cisco IOS версии 12.1 и позже, это значение скорости конфигурируемо. Представленная команда:

```
ip icmp rate-limit unreachable [DF] <1-4294967295 millisecond> no ip icmp rate-limit unreachable [DF] (DF limits rate for code=4)
```

См. идентификатор ошибки Cisco CSCdp28161 (только зарегистрированные клиенты) для получения дальнейшей информации.

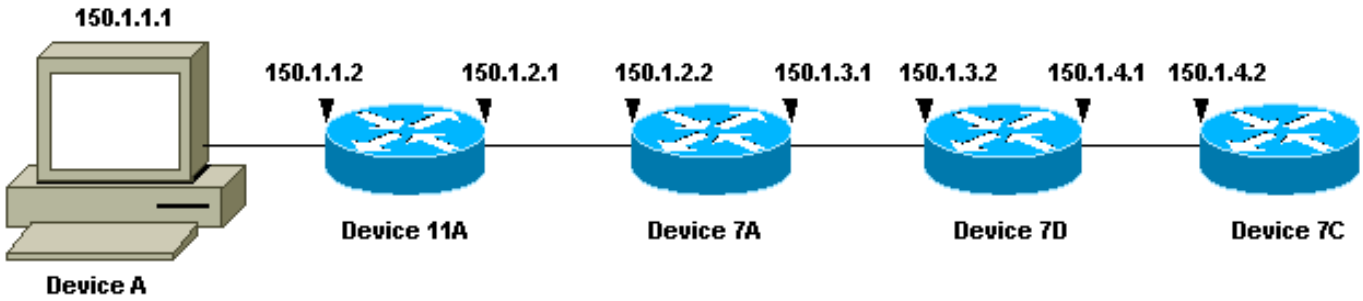
Это ограничение для скорости агрегации данных всего недостижимого ICMP, как показано в выходных данных ниже. См. RFC 792 для получения дополнительной информации.

```
type = 3, code
0 = net unreachable;
1 = host unreachable;
2 = protocol unreachable;
3 = port unreachable;
4 = fragmentation needed and DF set;
5 = source route failed.
```

Это ограничение не влияет на другие пакеты как сообщения "time exceeded"(превышение времени) ICMP или эхо-запросы протокола ICMP.

Примеры

Эта топология сети используется для примеров:



В каждом из этих трех примеров используется другое Устройство A. От Устройства A, **команда traceroute 150.1.4.2** выполняется к Устройству 7C.

В каждом из примеров **команда debug ip packet detail** работает на Устройстве 11 A.

Маршрутизатор Cisco с программным обеспечением Cisco IOS

Этот пример **команды расширенной трассировки** показывает варианты, которые можно

изменить при выполнении **команды traceroute** от маршрутизатора Cisco. В данном примере всему оставляют по умолчанию:

```
rp-10c-2611#traceroute Protocol [ip]: Target IP address: 150.1.4.2 Source address: 150.1.1.1
Numeric display [n]: Timeout in seconds [3]: Probe count [3]: Minimum Time to Live [1]: Maximum
Time to Live [30]: Port Number [33434]: Loose, Strict, Record, Timestamp, Verbose[none]: Type
escape sequence to abort. Tracing the route to 150.1.4.2 1 150.1.1.2 4 msec 0 msec 4 msec 2
150.1.2.2 4 msec 4 msec 0 msec 3 150.1.3.2 0 msec 0 msec 4 msec 4 150.1.4.2 4 msec * 0 msec rp-
11a-7204# *Dec 29 13:13:57.060: IP: s=150.1.1.2 (local), d=150.1.1.1 (Ethernet4/0), len 56,
sending *Dec 29 13:13:57.060: ICMP type=11, code=0 *Dec 29 13:13:57.064: IP: s=150.1.1.2
(local), d=150.1.1.1 (Ethernet4/0), len 56, sending *Dec 29 13:13:57.064: ICMP type=11, code=0
*Dec 29 13:13:57.064: IP: s=150.1.1.2 (local), d=150.1.1.1 (Ethernet4/0), len 56, sending *Dec
29 13:13:57.068: ICMP type=11, code=0
```

В этих выходных данных отладки Устройство 11 A передает сообщения "time exceeded"(превышение времени) ICMP к источнику зондов (150.1.1.1). Эти сообщения ICMP в ответ на начальные зонды, которые имели TTL=1. Устройство 11 A постепенно уменьшает TTL для обнуления и отвечает сообщениями "time exceeded"(превышение времени).

Примечание: Вы не видите зонды UDP в этих выходных данных отладки по двум причинам:

- Устройство 11 A не является назначением зондов UDP.
- TTL постепенно уменьшен для обнуления, и пакет никогда не маршрутизируется. Поэтому отладка никогда не распознает пакет.

```
*Dec 29 13:13:57.068: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0),
g=150.1.2.2, len 28, forward *Dec 29 13:13:57.068: UDP src=40309, dst=33437 *Dec 29
13:13:57.068: IP: s=150.1.2.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len
56, forward *Dec 29 13:13:57.068: ICMP type=11, code=0 *Dec 29 13:13:57.072: IP: s=150.1.1.1
(Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 28, forward *Dec 29
13:13:57.072: UDP src=37277, dst=33438 *Dec 29 13:13:57.072: IP: s=150.1.2.2
(FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29
13:13:57.072: ICMP type=11, code=0 *Dec 29 13:13:57.076: IP: s=150.1.1.1 (Ethernet4/0),
d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 28, forward *Dec 29 13:13:57.076: UDP
src=36884, dst=33439 *Dec 29 13:13:57.076: IP: s=150.1.2.2 (FastEthernet0/0), d=150.1.1.1
(Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 13:13:57.076: ICMP type=11, code=0
```

Эти выходные данные отладки показывают зонд UDP из источника 150.1.1.1 предназначенных к 150.1.4.2.

Примечание: В этих зондах TTL=2 (это не может быть замечено с отладкой). Устройство 11 A постепенно уменьшает TTL к 1 и вперед пакеты UDP на Устройство 7 A. Устройство 7 A постепенно уменьшает TTL для обнуления и отвечает сообщениями "time exceeded"(превышение времени) ICMP.

```
*Dec 29 13:13:57.080: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2,
len 28, forward *Dec 29 13:13:57.080: UDP src=37479, dst=33440 *Dec 29 13:13:57.080: IP:
s=150.1.3.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29
13:13:57.080: ICMP type=11, code=0 *Dec 29 13:13:57.084: IP: s=150.1.1.1 (Ethernet4/0),
d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 28, forward *Dec 29 13:13:57.084: UDP src=40631,
dst=33441 *Dec 29 13:13:57.084: IP: s=150.1.3.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0),
g=150.1.1.1, len 56, forward *Dec 29 13:13:57.084: ICMP type=11, code=0 *Dec 29 13:13:57.084:
IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 28, forward *Dec
29 13:13:57.088: UDP src=39881, dst=33442 *Dec 29 13:13:57.088: IP: s=150.1.3.2
(FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 13:13:57.088:
ICMP type=11, code=0
```

Вы видите следующие три зонда UDP в этих выходных данных отладки. TTL для этих зондов равняется 3. Устройство 11 A постепенно уменьшает TTL к 2 и вперед их на Устройстве 7 A. Устройство 7 A постепенно уменьшают TTL к 1 и передают пакеты на Устройстве 7B, который постепенно уменьшает TTL для обнуления и отвечает

сообщениями "time exceeded"(превышение времени) ICMP.

```
*Dec 29 13:13:57.088: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2,
len 28, forward *Dec 29 13:13:57.088: UDP src=39217, dst=33443 *Dec 29 13:13:57.092: IP:
s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29
13:13:57.092: ICMP type=3, code=3 *Dec 29 13:13:57.092: IP: s=150.1.1.1 (Ethernet4/0),
d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 28, forward *Dec 29 13:13:57.096: UDP src=34357,
dst=33444 *Dec 29 13:14:00.092: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0),
g=150.1.2.2, len 28, forward *Dec 29 13:14:00.092: UDP src=39587, dst=33445 *Dec 29
13:14:00.092: IP: s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56,
forward *Dec 29 13:14:00.092: ICMP type=3, code=3
```

Вы видите последние три зонда UDP в этих выходных данных отладки. Исходный TTL этих зондов равнялся 4. TTL был постепенно уменьшен к 3 Устройством 11 A, затем постепенно уменьшился к 2 Устройством 7 A, затем постепенно уменьшенных к 1 Устройством 7B. Устройство 7C отвечает сообщениями "port unreachable" ICMP, так как это было назначение зондов.

Примечание: Устройство 7C только передает два сообщения "port unreachable" ICMP из-за ограничения скорости.

ПК с Linux

```
[root#linux-pc]#traceroute -n 150.1.4.2 traceroute to 150.1.4.2 (150.1.4.2), 30 hops max, 40
byte packets 1. 150.1.1.2 1.140 ms 0.793 ms 0.778 ms 2. 150.1.2.2 2.213 ms 2.105 ms 3.491 ms 1.
150.1.3.2 3.146 ms 2.314 ms 2.347 ms 1. 150.1.4.2 3.579 ms * 2.954 ms rp-11a-7204# *Jan 2
07:17:27.894: IP: s=150.1.1.2 (local), d=150.1.1.1 (Ethernet4/0), len 56, sending *Jan 2
07:17:27.894: ICMP type=11, code=0 *Jan 2 07:17:27.894: IP: s=150.1.1.2 (local), d=150.1.1.1
(Ethernet4/0), len 56, sending *Jan 2 07:17:27.894: ICMP type=11, code=0 *Jan 2 07:17:27.894:
IP: s=150.1.1.2 (local), d=150.1.1.1 (Ethernet4/0), len 56, sending *Jan 2 07:17:27.894: ICMP
type=11, code=0
```

В этих выходных данных отладки Устройство 11 A передает сообщения "time exceeded"(превышение времени) ICMP к источнику зондов (150.1.1.1). Эти сообщения ICMP в ответ на начальные зонды, которые имели TTL=1. Устройство 11 A постепенно уменьшает TTL для обнуления и отвечает сообщениями "time exceeded"(превышение времени).

Примечание: Вы не видите зонды UDP в этих выходных данных отладки по двум причинам:

- Устройство 11 A не является назначением зондов UDP.
- TTL постепенно уменьшен для обнуления, и пакет никогда не маршрутизируется. Поэтому отладка никогда не распознает пакет.

```
*Jan 2 07:17:27.894: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2(FastEthernet0/0),
g=150.1.2.2, len 40, forward *Jan 2 07:17:27.894: UDP src=33302, dst=33438 *Jan 2
07:17:27.898: IP: s=150.1.2.2 (FastEthernet0/0), d=150.1.1.1(Ethernet4/0), g=150.1.1.1, len
56, forward *Jan 2 07:17:27.898: ICMP type=11, code=0 *Jan 2 07:17:27.898: IP: s=150.1.1.1
(Ethernet4/0), d=150.1.4.2(FastEthernet0/0), g=150.1.2.2, len 40, forward *Jan 2
07:17:27.898: UDP src=33302, dst=33439 *Jan 2 07:17:27.898: IP: s=150.1.2.2
(FastEthernet0/0), d=150.1.1.1(Ethernet4/0), g=150.1.1.1, len 56, forward *Jan 2
07:17:27.898: ICMP type=11, code=0 *Jan 2 07:17:27.898: IP: s=150.1.1.1 (Ethernet4/0),
d=150.1.4.2(FastEthernet0/0), g=150.1.2.2, len 40, forward *Jan 2 07:17:27.898: UDP
src=33302, dst=33440 *Jan 2 07:17:27.902: IP: s=150.1.2.2 (FastEthernet0/0),
d=150.1.1.1(Ethernet4/0), g=150.1.1.1, len 56, forward *Jan 2 07:17:27.902: ICMP type=11,
code=0
```

Примечание: В этих выходных данных отладки вы теперь видите зонд UDP из источника 150.1.1.1 предназначенных к 150.1.4.2.

Примечание: В этих зондах TTL=2 (это не может быть замечено с отладкой). Устройство 11

A постепенно уменьшает TTL к 1 и вперед пакеты UDP на Устройство 7 A. Устройство 7 A постепенно уменьшает TTL для обнуления и отвечает сообщениями "time exceeded"(превышение времени) ICMP.

```
*Jan 2 07:17:27.902: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2(FastEthernet0/0), g=150.1.2.2,
len 40, forward *Jan 2 07:17:27.902: UDP src=33302, dst=33441 *Jan 2 07:17:27.906: IP:
s=150.1.3.2 (FastEthernet0/0), d=150.1.1.1(Ethernet4/0), g=150.1.1.1, len 56, forward *Jan 2
07:17:27.906: ICMP type=11, code=0 *Jan 2 07:17:27.906: IP: s=150.1.1.1 (Ethernet4/0),
d=150.1.4.2(FastEthernet0/0), g=150.1.2.2, len 40, forward *Jan 2 07:17:27.906: UDP src=33302,
dst=33442 *Jan 2 07:17:27.910: IP: s=150.1.3.2 (FastEthernet0/0), d=150.1.1.1(Ethernet4/0),
g=150.1.1.1, len 56, forward *Jan 2 07:17:27.910: ICMP type=11, code=0 *Jan 2 07:17:27.910: IP:
s=150.1.1.1 (Ethernet4/0), d=150.1.4.2(FastEthernet0/0), g=150.1.2.2, len 40, forward *Jan 2
07:17:27.910: UDP src=33302, dst=33443 *Jan 2 07:17:27.910: IP: s=150.1.3.2 (FastEthernet0/0),
d=150.1.1.1(Ethernet4/0), g=150.1.1.1, len 56, forward *Jan 2 07:17:27.910: ICMP type=11, code=0
```

Следующие три зонда UDP теперь замечены в этих выходных данных отладки. TTL для этих зондов равняется 3. Устройство 11 A постепенно уменьшает TTL к 2 и вперед их на Устройстве 7 A. Устройство 7 A постепенно уменьшают TTL к 1 и передают пакеты на Устройстве 7B, который постепенно уменьшает TTL для обнуления и отвечает сообщениями "time exceeded"(превышение времени) ICMP.

```
*Jan 2 07:17:27.910: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2(FastEthernet0/0), g=150.1.2.2,
len 40, forward *Jan 2 07:17:27.910: UDP src=33302, dst=33444 *Jan 2 07:17:27.914: IP:
s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1(Ethernet4/0), g=150.1.1.1, len 56, forward *Jan 2
07:17:27.914: ICMP type=3, code=3 *Jan 2 07:17:27.914: IP: s=150.1.1.1 (Ethernet4/0),
d=150.1.4.2(FastEthernet0/0), g=150.1.2.2, len 40, forward *Jan 2 07:17:27.914: UDP src=33302,
dst=33445 *Jan 2 07:17:32.910: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2(FastEthernet0/0),
g=150.1.2.2, len 40, forward *Jan 2 07:17:32.910: UDP src=33302, dst=33446 *Jan 2 07:17:32.914:
IP: s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1(Ethernet4/0), g=150.1.1.1, len 56, forward *Jan 2
07:17:32.914: ICMP type=3, code=3
```

Эти выходные данные отладки показывают последние три зонда UDP. Исходный TTL этих зондов равнялся 4. TTL был постепенно уменьшен к 3 Устройством 11 A, затем постепенно уменьшился к 2 Устройством 7 A, затем постепенно уменьшенных к 1 Устройством 7B. Устройство 7C тогда отвечает сообщениями "port unreachable" ICMP, так как это было назначение зондов.

Примечание: Устройство 7C только передает два сообщения "port unreachable" ICMP из-за ограничения скорости.

ПК с MS Windows

```
C:\>tracert 150.1.4.2 1 <10 ms <10 ms <10 ms 10.1.1.2 1 <10 ms <10 ms <10 ms 10.1.2.2 1 <10 ms
<10 ms <10 ms 10.1.3.2 1 <10 ms 10 ms 10 ms 10.1.4.2 Trace complete rp-11a-7204# *Dec 29
14:02:22.236: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 78,
forward *Dec 29 14:02:22.236: UDP src=137, dst=137 *Dec 29 14:02:22.240: IP: s=150.1.4.2
(FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 14:02:22.240:
ICMP type=3, code=3 *Dec 29 14:02:23.732: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2
(FastEthernet0/0), g=150.1.2.2, len 78, forward *Dec 29 14:02:23.732: UDP src=137, dst=137 *Dec
29 14:02:23.736: IP: s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len
56, forward *Dec 29 14:02:23.736: ICMP type=3, code=3 *Dec 29 14:02:25.236: IP: s=150.1.1.1
(Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 78, forward *Dec 29 14:02:25.236:
UDP src=137, dst=137 *Dec 29 14:02:25.236: IP: s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1
(Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 14:02:25.240: ICMP type=3, code=3 *Dec 29
14:02:26.748: IP: s=150.1.1.2 (local), d=150.1.1.1 (Ethernet4/0), len 56, sending *Dec 29
14:02:26.748: ICMP type=11, code=0 *Dec 29 14:02:26.752: IP: s=150.1.1.2 (local), d=150.1.1.1
(Ethernet4/0), len 56, sending *Dec 29 14:02:26.752: ICMP type=11, code=0 *Dec 29 14:02:26.752:
IP: s=150.1.1.2 (local), d=150.1.1.1 (Ethernet4/0), len 56, sending *Dec 29 14:02:26.752: ICMP
type=11, code=0
```

В этих выходных данных отладки Устройство 11 A передает сообщения "time exceeded"(превышение времени) ICMP к источнику зондов (150.1.1.1). Эти сообщения ICMP в ответ на начальные зонды, которые являются пакетами эхо-запроса протокола ICMP с TTL=1. Устройство 11 A постепенно уменьшает TTL для обнуления и отвечает сообщениями ICMP.

Примечание: Наверху вы видите запросы ИМЕНИ NETBIOS. Эти запросы замечены как пакеты UDP с источником и портами назначения 137. По причинам ясности пакеты NETBIOS удалены из остатка выходных данных отладки. Можно использовать-*d* опцию в **команде tracert** для отключения поведения NETBIOS.

Примечание: Вы не видите Образцов ICMP в этих **выходных данных отладки** по двум причинам:

- Устройство 11 A не является назначением Образцов ICMP.
- TTL постепенно уменьшен для обнуления, и пакет никогда не маршрутизируется. Поэтому отладка никогда не распознает пакет.

***Dec 29 14:02:32.256: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:32.256: ICMP type=8, code=0 *Dec 29 14:02:32.260: IP: s=150.1.2.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 14:02:32.260: ICMP type=11, code=0** *Dec 29 14:02:32.260: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:32.260: ICMP type=8, code=0 *Dec 29 14:02:32.260: IP: s=150.1.2.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 14:02:32.260: ICMP type=11, code=0 *Dec 29 14:02:32.264: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:32.264: ICMP type=8, code=0 *Dec 29 14:02:32.264: IP: s=150.1.2.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 14:02:32.264: ICMP type=11, code=0

В этих выходных данных отладки вы теперь видите Образца ICMP из источника 150.1.1.1 предназначенных к 150.1.4.2.

Примечание: В этих зондах, TTL=2 (это не может быть замечено с отладкой). Устройство 11 A постепенно уменьшает TTL к 1 и вперед пакеты UDP на Устройстве 7 A. Устройство 7 A постепенно уменьшает TTL для обнуления и отвечает сообщениями "time exceeded"(превышение времени) ICMP.

***Dec 29 14:02:37.776: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:37.776: ICMP type=8, code=0 *Dec 29 14:02:37.776: IP: s=150.1.3.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 14:02:37.776: ICMP type=11, code=0** *Dec 29 14:02:37.780: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:37.780: ICMP type=8, code=0 *Dec 29 14:02:37.780: IP: s=150.1.3.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 14:02:37.780: ICMP type=11, code=0 *Dec 29 14:02:37.780: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:37.780: ICMP type=8, code=0 *Dec 29 14:02:37.784: IP: s=150.1.3.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 56, forward *Dec 29 14:02:37.784: ICMP type=11, code=0

Вы видите следующие трех Образцов ICMP в этих выходных данных отладки. TTL для этих зондов равняется 3. Устройство 11 A постепенно уменьшает TTL к 2 и вперед их на Устройстве 7 A. Устройство 7 A постепенно уменьшают TTL к 1 и передают пакеты на Устройстве 7B, который постепенно уменьшает TTL для обнуления и отвечает сообщениями "time exceeded"(превышение времени) ICMP.

***Dec 29 14:02:43.292: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:43.292: ICMP type=8, code=0 *Dec 29 14:02:43.296: IP: s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 92, forward *Dec 29 14:02:43.296:**

ICMP type=0, code=0 *Dec 29 14:02:43.296: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:43.296: ICMP type=8, code=0 *Dec 29 14:02:43.300: IP: s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 92, forward *Dec 29 14:02:43.300: ICMP type=0, code=0 *Dec 29 14:02:43.300: IP: s=150.1.1.1 (Ethernet4/0), d=150.1.4.2 (FastEthernet0/0), g=150.1.2.2, len 92, forward *Dec 29 14:02:43.300: ICMP type=8, code=0 *Dec 29 14:02:43.304: IP: s=150.1.4.2 (FastEthernet0/0), d=150.1.1.1 (Ethernet4/0), g=150.1.1.1, len 92, forward *Dec 29 14:02:43.304: ICMP type=0, code=0

Эти выходные данные отладки показывают последние трех Образцов ICMP. Исходный TTL этих зондов равнялся 4. TTL был постепенно уменьшен к 3 Устройством 11 A, затем постепенно уменьшился к 2 Устройством 7 A, затем постепенно уменьшенных к 1 Устройством 7B. Устройство 7C тогда отвечает Сообщениями с эхо-ответом ICMP (type=0, code=0), так как это было назначение зондов.

Примечание: Сообщения с эхо-ответом ICMP не являются скоростью, ограниченной, как сообщения "port unreachable" ICMP были. В этом случае вы видите все три передаваемые Сообщения с эхо-ответом ICMP.

Дополнительные примечания

В маршрутизаторах Cisco коды для ответа **команды traceroute**:

```
! -- success
* -- time out
N -- network unreachable
H -- host unreachable
P -- protocol unreachable
A -- admin denied
Q -- source quench received (congestion)
? -- unknown (any other ICMP message)
```

При выполнении **команды traceroute** от UNIX обратите внимание на эти элементы:

- Можно получить "traceroute: сокет ICMP: Разрешения запретили" сообщения.
- **Программа трассировки** полагается на Network Interface Tap (NIT) для отслеживания в сети. Это устройство только доступно root. Необходимо или выполнить программу как root или установить идентификатор пользователя для root.

Сводка

Этот документ продемонстрировал, как **команда traceroute** определяет путь, который пакет берет от данного источника до заданного получателя с использованием UDP и пакетов ICMP. Возможные типы сообщений ICMP в выходных данных:

- Если TTL превышен в пути, type=11, code=0, то пакет передает обратно транзитный маршрутизатор во всех случаях, где TTL тестовых пакетов истекает, прежде чем пакеты достигают назначения.
- Если порт недостижим, type=3, code=3, то пакет передают обратно в ответ на тестовые пакеты UDP, когда они достигают назначения (приложение UDP не определено). Эти пакеты ограничены одним пакетом на 500 мс. Это объясняет, почему ответ от назначения (см. выходные данные для маршрутизатора Cisco и Linux), подведенный в ровных ответах. Устройство 7C не генерирует сообщение ICMP, и выходные данные **команды traceroute** в каждом устройстве ждут в течение нескольких секунд. В случае выходных данных **команды tracert** MS Windows генерируется сообщение ICMP, потому

что порт 137 UDP не существует в маршрутизаторе Cisco.
- Если существует эхо, type=8, code=0, то пакет тестового эха - пакета передан ПК MS Windows.
- Если существует эхо - ответ, type=0, code=0, то ответ на предыдущий пакет передается, когда достигнуто назначение. Это только применяется к **команде tracert** MS Windows.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация