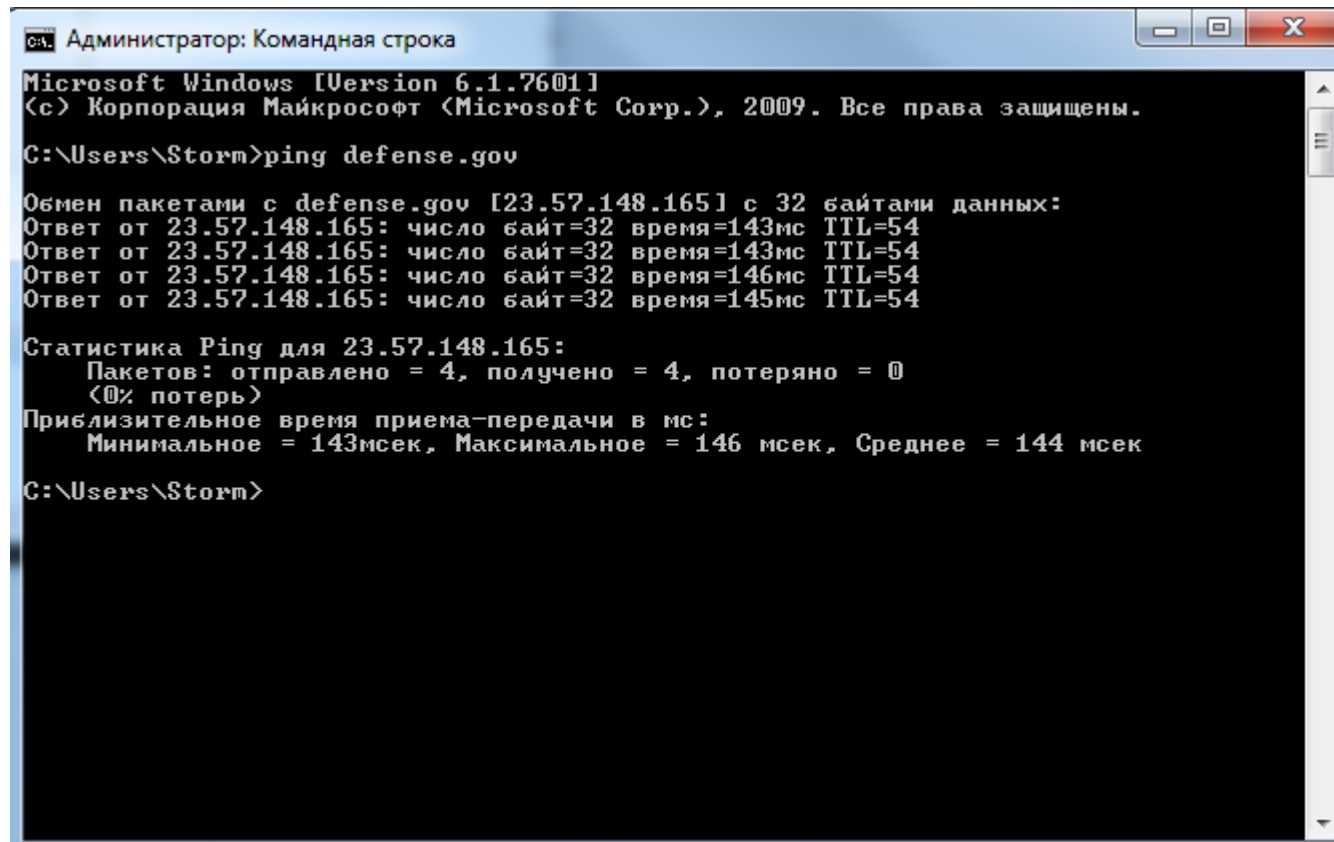


Команда ping.

Команда ping (Packet InterNet Groper) является очень распространенным средством для устранения неполадок, связанных с доступом к устройствам. В ней для определения активности удаленного хоста используются два типа сообщений протокола ICMP – ECHO REQUEST(в заголовке ICMP сообщения код типа равен 8) и ECHO REPLY (код типа в ICMP-заголовке равен 0). Команда ping также измеряет количество времени, необходимого для получения эхо-ответа. Команда ping сначала посылает пакет эхо-запроса на адрес, а затем ожидает ответа. В поле данных отправляемого icmp-пакета обычно содержатся символы английского алфавита. В ответ на такой запрос, опрашиваемый узел должен отправить icmp-пакет с теми же данными, которые были приняты. Эхо-тест является удачным только в том случае, если ECHO REQUEST попадает в место назначения, и место назначения может отправить ECHO REPLY к источнику эхо-теста в течение заданного временного интервала. Отсутствие эхо-ответа не всегда является признаком неисправности, поскольку иногда по соображениям безопасности, некоторые узлы настраиваются на игнорирование эхо-запросов, посылаемых PING.



```
Администратор: Командная строка
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Storm>ping defense.gov

Обмен пакетами с defense.gov [23.57.148.165] с 32 байтами данных:
Ответ от 23.57.148.165: число байт=32 время=143мс TTL=54
Ответ от 23.57.148.165: число байт=32 время=143мс TTL=54
Ответ от 23.57.148.165: число байт=32 время=146мс TTL=54
Ответ от 23.57.148.165: число байт=32 время=145мс TTL=54

Статистика Ping для 23.57.148.165:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 143мсек, Максимальное = 146 мсек, Среднее = 144 мсек

C:\Users\Storm>
```

*Беспроводное сетевое соединение

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|------------|--------------|--------------|-------------|----------|---------------------|--|
| 606.172270 | 192.168.1.65 | defense.gov | ICMP | 74 | Echo (ping) request | id=0x0001, seq=1/256, ttl=128 (reply in 22067) |
| 606.316004 | defense.gov | 192.168.1.65 | ICMP | 74 | Echo (ping) reply | id=0x0001, seq=1/256, ttl=54 (request in 22065) |
| 607.173120 | 192.168.1.65 | defense.gov | ICMP | 74 | Echo (ping) request | id=0x0001, seq=2/512, ttl=128 (reply in 22071) |
| 607.316395 | defense.gov | 192.168.1.65 | ICMP | 74 | Echo (ping) reply | id=0x0001, seq=2/512, ttl=54 (request in 22070) |
| 608.173146 | 192.168.1.65 | defense.gov | ICMP | 74 | Echo (ping) request | id=0x0001, seq=3/768, ttl=128 (reply in 22073) |
| 608.319758 | defense.gov | 192.168.1.65 | ICMP | 74 | Echo (ping) reply | id=0x0001, seq=3/768, ttl=54 (request in 22072) |
| 609.173113 | 192.168.1.65 | defense.gov | ICMP | 74 | Echo (ping) request | id=0x0001, seq=4/1024, ttl=128 (reply in 22076) |
| 609.318114 | defense.gov | 192.168.1.65 | ICMP | 74 | Echo (ping) reply | id=0x0001, seq=4/1024, ttl=54 (request in 22074) |

Frame 22065: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{67CFF121-D998-4...}

Ethernet II, Src: ZyxelCom_ff:74:00 (fc:f5:28:ff:74:00), Dst: KEENETIC-0668 (50:ff:20:a6:1a:1e)

Internet Protocol Version 4, Src: 192.168.1.65 (192.168.1.65), Dst: defense.gov (23.57.148.165)

- 0100 = Version: 4
- ... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 60
- Identification: 0x48aa (18602)
- 000. = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: ICMP (1)
- Header Checksum: 0x844f [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.65 (192.168.1.65)
- Destination Address: defense.gov (23.57.148.165)

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d5a [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Response frame: 22067]

Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]

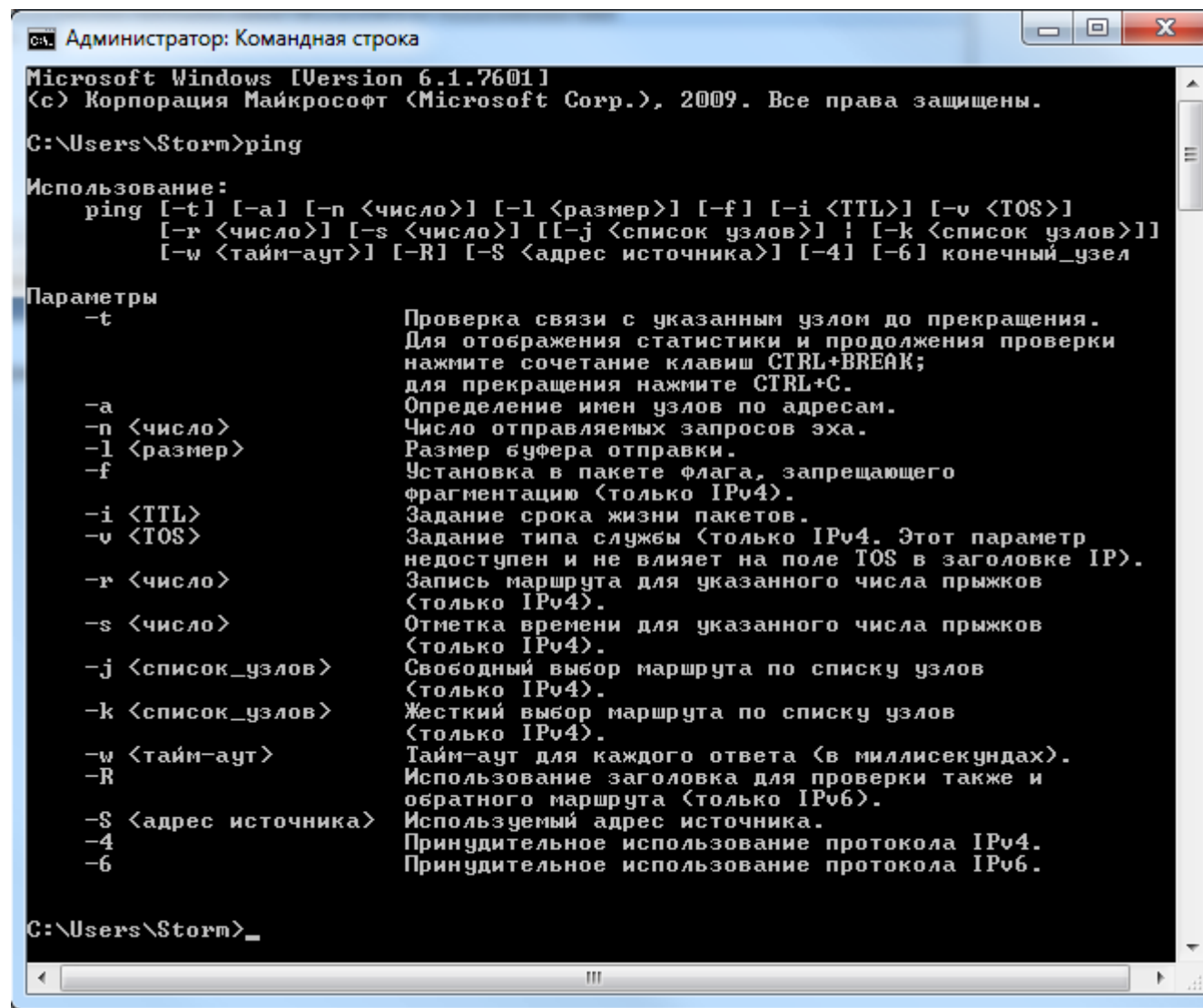
ff 20 a6 1a 1e fc f5 28 ff 74 00 08 00 45 00 P (. t . . . E .
3c 48 aa 00 00 80 01 84 4f c0 a8 01 41 17 39 < H 0 . . . A . 9
a5 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 M Z abcdef
68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
61 62 63 64 65 66 67 68 69 wabcdefg hi

Data (data.data), 32 байта

Пакеты: 23488 · Показаны: 8 (0.0%)

Профиль: Default

Команда ping может быть вызвана с параметрами:



```
Администратор: Командная строка
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Storm>ping

Использование:
ping [-t] [-a] [-n <число>] [-l <размер>] [-f] [-i <TTL>] [-v <TOS>]
  [-r <число>] [-s <число>] [[-j <список узлов>] ! [-k <список узлов>]]
  [-w <тайм-аут>] [-R] [-S <адрес источника>] [-4] [-6] конечный_узел

Параметры
-t          Проверка связи с указанным узлом до прекращения.
            Для отображения статистики и продолжения проверки
            нажмите сочетание клавиш CTRL+BREAK;
            для прекращения нажмите CTRL+C.
-a          Определение имен узлов по адресам.
-n <число>  Число отправляемых запросов эха.
-l <размер>  Размер буфера отправки.
-f          Установка в пакете флага, запрещающего
            фрагментацию (только IPv4).
-i <TTL>     Задание срока жизни пакетов.
-v <TOS>     Задание типа службы (только IPv4. Этот параметр
            недоступен и не влияет на поле TOS в заголовке IP).
-r <число>   Запись маршрута для указанного числа прыжков
            (только IPv4).
-s <число>   Отметка времени для указанного числа прыжков
            (только IPv4).
-j <список_узлов> Свободный выбор маршрута по списку узлов
            (только IPv4).
-k <список_узлов> Жесткий выбор маршрута по списку узлов
            (только IPv4).
-w <тайм-аут> Тайм-аут для каждого ответа (в миллисекундах).
-R          Использование заголовка для проверки также и
            обратного маршрута (только IPv6).
-S <адрес источника> Используемый адрес источника.
-4          Принудительное использование протокола IPv4.
-6          Принудительное использование протокола IPv6.

C:\Users\Storm>
```

Вызов команды ping с параметром -r <число> - отображает маршрут для указанного числа переходов.

```
Администратор: Командная строка

C:\Users\Storm>ping -r 9 yandex.ru

Обмен пакетами с yandex.ru [77.88.44.55] с 32 байтами данных:
Ответ от 77.88.44.55: число байт=32 время=96мс TTL=58
    Маршрут: 46.45.193.210 ->
              185.140.148.107 ->
              185.140.148.106 ->
              94.25.47.121 ->
              94.25.47.122 ->
              87.250.246.131 ->
              37.9.121.254 ->
              10.24.4.1 ->
              0.0.0.0
Ответ от 77.88.44.55: число байт=32 время=63мс TTL=58
    Маршрут: 46.45.193.210 ->
              185.140.148.107 ->
              185.140.148.106 ->
              94.25.47.121 ->
              94.25.47.122 ->
              87.250.246.131 ->
              37.9.121.254 ->
              10.24.4.1 ->
              0.0.0.0
Ответ от 77.88.44.55: число байт=32 время=54мс TTL=58
    Маршрут: 46.45.193.210 ->
              185.140.148.107 ->
              185.140.148.106 ->
              94.25.47.121 ->
              94.25.47.122 ->
              87.250.246.131 ->
              37.9.121.254 ->
              10.24.4.1 ->
              0.0.0.0
Ответ от 77.88.44.55: число байт=32 время=174мс TTL=58
    Маршрут: 46.45.193.210 ->
              185.140.148.107 ->
              185.140.148.106 ->
              94.25.47.121 ->
              94.25.47.122 ->
              87.250.246.131 ->
              37.9.121.254 ->
              10.24.4.1 ->
              0.0.0.0

Статистика Ping для 77.88.44.55:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
Приблизительное время приема-передачи в мс:
    Минимальное = 54мсек, Максимальное = 174 мсек, Среднее = 96 мсек

C:\Users\Storm>_
```

Нужно учитывать тот факт, что в версии утилиты ping.exe для Windows, число переходов может принимать значение от 1 до 9. В случаях, когда этого значения недостаточно, используется команда tracert.

Команда tracert

Tracert позволяет сделать трассировку маршрута до заданного узла в локальной сети или сети Интернет. Команда tracert также как и команда ping использует сообщения протокола ICMP, но использует постепенное увеличение значения в поле TTL(Time To Live) заголовка IP пакета до тех пор пока пакет не достигнет целевого хоста. Сначала на хост назначения посылаются три пакета с полем TTL установленным в значение 1. При достижении первого маршрутизатора в цепочке он вычитает из поля TTL единицу и проверяет полученное значение счетчика TTL. Оно становится равным нулю, маршрутизатор отбрасывает этот пакет и отправляет ICMP сообщение отправителю о превышении времени жизни (сообщение "Time Exceeded", значение 0x11 в заголовке ICMP). При получении такого сообщения от маршрутизатора его IP – адрес заносится в таблицу маршрута. Затем процедура повторяется но TTL устанавливается равным 2 – первый маршрутизатор его уменьшит до 1 и отправит следующему в цепочке, который после вычитания 1 обнулит TTL и сообщит о превышении времени жизни. Таким образом будет получен второй IP – адрес узла участвующего в доставке пакета до хоста назначения. Данная процедура будет продолжаться до тех пор пока не будет достигнут конечный узел или до обнаружении неисправности, не позволяющей доставить пакет. Помимо IP – адреса узла в строку вывода также записывается время его ответа по каждому из трех отправленных на него пакетов.

```
Администратор: Командная строка

Трассировка завершена.

C:\Windows\system32>tracert -4 defense.gov

Трассировка маршрута к defense.gov [23.57.148.165]
с максимальным числом прыжков 30:

  1  <1 мс    <1 мс    <1 мс    KEENETIC-0668 [192.168.1.1]
  2   1 ms     1 ms     1 ms     100.105.0.1
  3   1 ms     1 ms     5 ms     185.140.148.106
  4  44 ms    38 ms    37 ms    188.128.126.51
  5  59 ms    40 ms    40 ms    sto-b2-link.ip.twelve99.net [80.239.128.74]
  6  38 ms    38 ms    38 ms    sto-bb2-link.ip.twelve99.net [62.115.140.216]
  7   *        64 ms    *        kbn-bb6-link.ip.twelve99.net [62.115.139.173]
  8   *        *        128 ms   ewr-bb2-link.ip.twelve99.net [80.91.254.91]
  9  132 ms   131 ms   137 ms   bost-b4-link.ip.twelve99.net [62.115.138.59]
 10  141 ms   131 ms   131 ms   bost-b3-link.ip.twelve99.net [62.115.139.191]
 11  130 ms   131 ms   135 ms   akamai-ic-384688.ip.twelve99-cust.net [62.115.159.249]
 12  146 ms   147 ms   321 ms   ae2.ecx-bos3.netarch.akamai.com [23.203.149.133]
 13  141 ms   146 ms   146 ms   a23-57-148-165.deploy.static.akamaitechnologies.com [23.57.148.165]

Трассировка завершена.

C:\Windows\system32>
```

Захват из Беспроводная сеть

ФайлПравкаВидЗапускЗахватАнализСтатистикаТелефонияБеспроводная связьИнструментыСправка

icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-----------------|---------------|----------|--------|--|
| 4851 | 39.013464 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=346/23041, ttl=1 (no response found!) |
| 4852 | 39.015477 | 192.168.1.1 | 192.168.1.45 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in transit) |
| 4853 | 39.016095 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=347/23297, ttl=1 (no response found!) |
| 4854 | 39.016776 | 192.168.1.1 | 192.168.1.45 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in transit) |
| 4855 | 39.017248 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=348/23553, ttl=1 (no response found!) |
| 4856 | 39.017943 | 192.168.1.1 | 192.168.1.45 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in transit) |
| 4957 | 40.542860 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=349/23809, ttl=2 (no response found!) |
| 4958 | 40.544973 | 100.105.0.1 | 192.168.1.45 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in transit) |
| 4959 | 40.547317 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=350/24065, ttl=2 (no response found!) |
| 4960 | 40.548718 | 100.105.0.1 | 192.168.1.45 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in transit) |
| 4961 | 40.549947 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=351/24321, ttl=2 (no response found!) |
| 4962 | 40.551640 | 100.105.0.1 | 192.168.1.45 | ICMP | 134 | Time-to-live exceeded (Time to live exceeded in transit) |
| 5071 | 46.577659 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=352/24577, ttl=3 (no response found!) |
| 5072 | 46.579460 | 185.140.148.106 | 192.168.1.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 5073 | 46.580523 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=353/24833, ttl=3 (no response found!) |
| 5074 | 46.582480 | 185.140.148.106 | 192.168.1.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 5075 | 46.583099 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=354/25089, ttl=3 (no response found!) |
| 5076 | 46.584637 | 185.140.148.106 | 192.168.1.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 5179 | 52.605639 | 192.168.1.45 | 23.57.148.165 | ICMP | 106 | Echo (ping) request id=0x0001, seq=355/25345, ttl=4 (no response found!) |
| 5180 | 52.648628 | 188.128.126.51 | 192.168.1.45 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.45

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

Total Length: 120

Identification: 0xe34a (58186)

> 000. = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: ICMP (1)

Header Checksum: 0x12fc [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.1

Destination Address: 192.168.1.45

[Stream index: 9]

Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

Checksum: 0xf4ff [correct]

[Checksum Status: Good]

0000 44 6d 57 bc a2 7c 50 ff 20 a6 1a 1e 08 00 45 c0

0010 00 78 e3 4a 00 00 40 01 12 fc c0 a8 01 01 c0 a8

0020 01 2d 0b 00 f4 ff 00 00 00 00 45 00 00 5c 05 e4

0030 00 00 01 01 46 0a c0 a8 01 2d 17 39 94 a5 08 00

0040 f6 a4 00 01 01 5a 00 00 00 00 00 00 00 00 00

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0080 00 00 00 00 00 00

