Usar o comando traceroute nos sistemas operacionais

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)
- [Conventions](#)

[Informações de Apoio](#)

[Operação geral](#)

- [Cisco IOS e Linux](#)
- [Microsoft Windows](#)

[Limitação da taxa de mensagens que não chegam ao seu destino do ICMP](#)

[Examples](#)

- [Roteador Cisco com software Cisco IOS](#)
- [PC com Linux](#)
- [PC executando o MS Windows](#)

[Notas adicionais](#)

[Summary](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como o comando traceroute opera em sistemas diferentes.

Pré-requisitos

Requisitos

Os leitores deste documento devem ter conhecimento básico de um destes sistemas operacionais:

- Cisco IOS® Software
- Linux
- Microsoft Windows

Componentes Utilizados

As informações neste documento se aplicam a estas versões de software e hardware:

- Roteador Cisco que executa o Cisco IOS Software Release 12
- PC com Red Hat Linux
- PC que executa o MS Windows

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

O comando traceroute permite determinar o caminho que um pacote percorre para chegar a um destino de uma determinada origem, retornando a sequência de saltos que o pacote percorreu. Esse utilitário é fornecido com o sistema operacional do host (por exemplo, Linux ou Microsoft (MS) Windows), bem como com o software Cisco IOS.

Operação geral

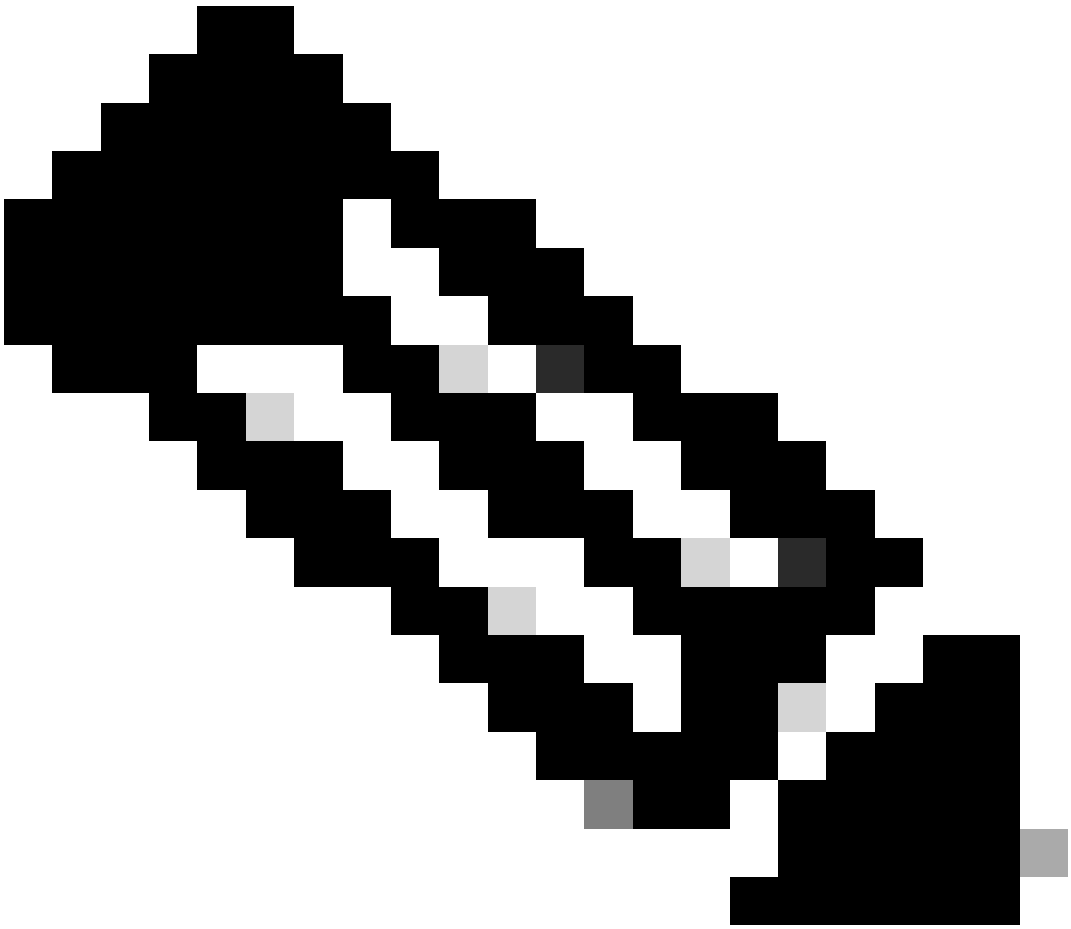
Se você executar o comando traceroute ip-address em um dispositivo de origem (como um host ou um roteador que atua como um host), ele enviará pacotes IP para o destino com valores Time To Live (TTL) que incrementam até a contagem máxima de saltos especificada. Esse valor é 30 por padrão. Normalmente, cada roteador no caminho para o destino diminui o valor do campo TTL em uma unidade enquanto encaminha esses pacotes. Quando um roteador no meio do caminho encontra um pacote com TTL = 1, responde com uma mensagem de "tempo excedido" do Internet Control Message Protocol (ICMP) para a origem. Essa mensagem informa à origem que o pacote atravessou esse roteador específico como salto

Há algumas diferenças na forma como o comando traceroute é implementado nos vários sistemas operacionais abordados neste documento.

Cisco IOS e Linux

O TTL para a prova de datagrama inicial do protocolo UDP é definido como 1 (ou o TTL mínimo, conforme especificado pelo usuário no traceroute comando estendido. A porta UDP de destino da sonda de datagrama inicial é definida como 33434 (ou como especificado na saída do traceroute comando estendido). O comando estendido traceroute é uma variação do comando traceroute traceroute ordinário que permite que os valores padrão dos parâmetros usados pela operação, como o TTL e o número de porta de destino, sejam modificados. Para obter mais informações sobre como

usar o traceroute comando estendido, consulte Compreender os Comandos ping e traceroute estendidos. A porta UDP de origem da sondagem de datagrama inicial é aleatória e tem OR do operador lógico com 0x8000 (garante uma porta de origem mínima de 0x8000). Essas etapas ilustram o que acontece quando o datagrama UDP é iniciado:



Note: Os parâmetros são configuráveis. Este exemplo começa com n = 1 e termina com n = 3.

---

1. O datagrama UDP é despachado com TTL = 1, a porta UDP de destino = 33434 e a porta de origem é aleatória.
2. A porta de destino UDP é incrementada, a porta UDP de origem é aleatória e o segundo datagrama é despachado.
3. A Etapa 2 é repetida para até três testes (ou quantas vezes forem solicitadas em uma saída de traceroute comando estendido). Para cada uma das sondagens enviadas, você recebe uma mensagem de "TTL excedido", que é usada para criar um caminho passo a passo para o

host de destino.

4. O TTL é incrementado e esse ciclo se repete com números de porta de destino incrementais, se a mensagem de tempo excedido ICMP for recebida. Você também pode obter uma destas mensagens:

    - Uma mensagem ICMP tipo 3, código 3 (destino inalcançável, porta inalcançável), que indica que um host foi alcançado.
    - Um host inalcançável, rede inalcançável, TTL máximo excedido ou um tipo de mensagem de timeout, o que significa que o teste está sendo reenviado.

Os roteadores Cisco enviam pacotes de sondagem UDP com uma porta de origem aleatória e uma porta de destino incremental (para distinguir as diferentes sondagens). Os roteadores Cisco enviam o tempo de mensagem ICMP excedido de volta à origem de onde o pacote UDP/ICMP foi recebido.

O comando Linux `traceroute` é semelhante à implementação do roteador Cisco. No entanto, ele usa uma porta de origem fixa. A `-n` opção no `traceroute` comando é usada para evitar uma solicitação a um servidor de nomes.

Microsoft Windows

O`tracert`comando MS Windows usa datagramas de solicitação de eco ICMP em vez de datagramas UDP como sondas. As solicitações de eco ICMP são iniciadas com o incremento de TTL e ocorre a mesma operação conforme descrito em Cisco IOS e Linux. O significado de usar datagramas de solicitação de eco ICMP é que o salto final não depende da resposta de uma mensagem ICMP inalcançável do host de destino. Em vez disso, depende de uma mensagem de resposta de eco ICMP.

A sintaxe do comando é:

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

Esta tabela explica os parâmetros do comando:

Parâmetro	Descrição
-d	Especifica a não resolução de endereços para nomes de computador.
-h maximum_hops	Especifica o número máximo de saltos para pesquisar um destino.
-j computer-list	Especifica uma rota de origem livre ao longo da lista de computadores.
-w timeout	Aguarda o número de milissegundos especificado pelo limite de tempo para cada resposta.
target_name	Nome do computador de destino.

Limitação da taxa de mensagens que não chegam ao seu destino do ICMP

Os valores inacessíveis do ICMP são limitados a um pacote por 500 ms, como uma proteção contra ataques de negação de serviço (DoS), em um roteador Cisco. No software Cisco IOS versão 12.1 e posterior, esse valor de taxa é configurável. O comando apresentado é:

<#root>

Router(config)#

ip icmp rate-limit unreachable ?

```
  <1-4294967295>  Once per milliseconds
  DF              code 4, fragmentation needed and DF set
```

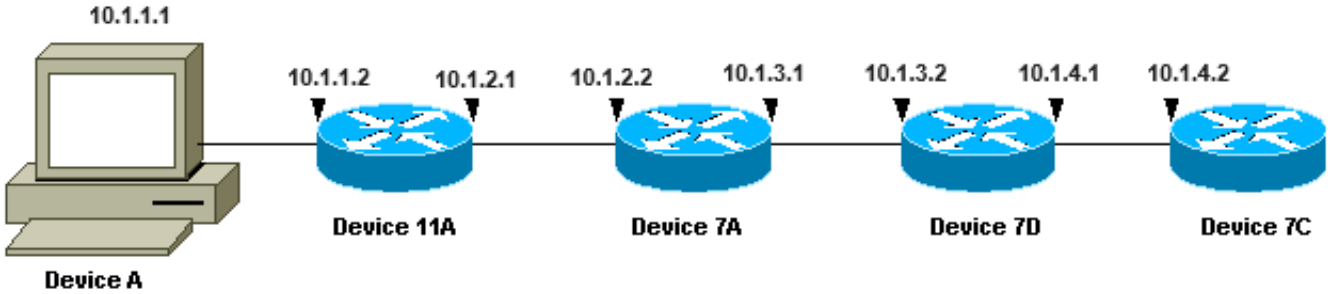
Essa limitação é para a taxa de agregação de todos os valores inacessíveis do ICMP, conforme mostra essa saída. Consulte a RFC 792 para obter mais informações.

```
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.
```

Essa limitação não afeta outros pacotes, como solicitações de eco ICMP ou mensagens de tempo excedido ICMP.

Examples

Esta topologia de rede é usada para os exemplos:



Topologia de rede

Em cada um dos três exemplos, um dispositivo A diferente é usado. No Dispositivo A, o comando traceroute 10.1.4.2 é executado no Dispositivo 7C.

Em cada um dos exemplos, o comando debug ip packet detail é executado no Dispositivo 11A.

Roteador Cisco com software Cisco IOS

Este exemplo de traceroute comando estendido mostra as opções que você pode alterar ao executar um traceroute comando a partir de um roteador Cisco. Neste exemplo, tudo é deixado como padrão:

<#root>

```
rp-10c-2611#
```

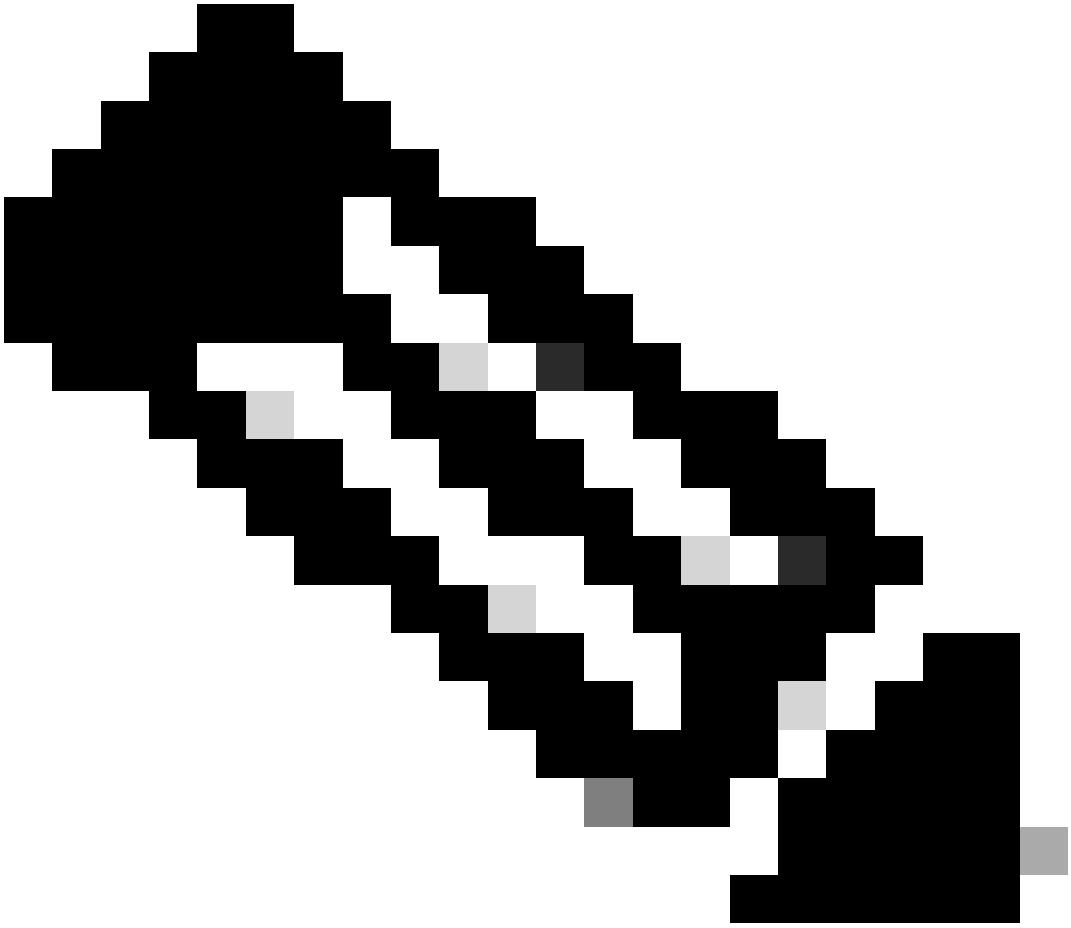
traceroute

```
Protocol [ip]:
Target IP address: 10.1.4.2
Source address: 10.1.1.1
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 10.1.4.2

1 10.1.1.2 4 msec 0 msec 4 msec
2 10.1.2.2 4 msec 4 msec 0 msec
3 10.1.3.2 0 msec 0 msec 4 msec
4 10.1.4.2 4 msec * 0 msec


rp-11a-7204#
```

***Dec 29 13:13:57.060: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),**
len 56, sending
***Dec 29 13:13:57.060: ICMP type=11, code=0**

```
*Dec 29 13:13:57.064: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),
 len 56, sending
*Dec 29 13:13:57.064: ICMP type=11, code=0
*Dec 29 13:13:57.064: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),
 len 56, sending
*Dec 29 13:13:57.068: ICMP type=11, code=0
```

Nesta saída de depuração, o Dispositivo 11A envia mensagens de tempo excedido ICMP à origem dos testadores (10.1.1.1). Essas mensagens ICMP são em resposta às sondas iniciais que tinham um TTL=1. O dispositivo 11A diminui o TTL para zero e responde com as mensagens de tempo excedido.



Note: Você não vê os testes UDP nesta saída de depuração por duas razões:

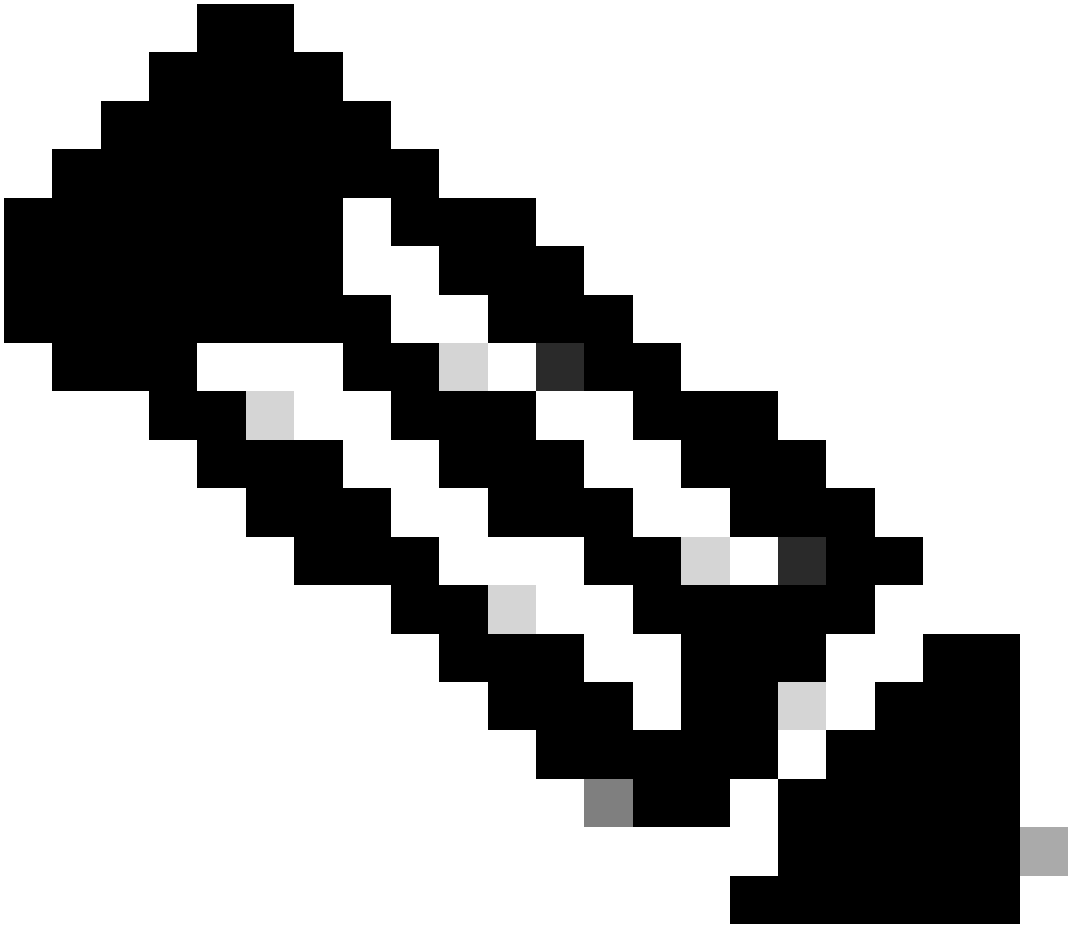
- O dispositivo 11A não é o destino das sondagens UDP.
- O TTL é reduzido para zero e o pacote nunca é encaminhado. Portanto, a depuração nunca reconhece o pacote.

<#root>

```
*Dec 29 13:13:57.068: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:13:57.068: UDP src=40309, dst=33437
*Dec 29 13:13:57.068: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 13:13:57.068: ICMP type=11, code=0

*Dec 29 13:13:57.072: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:13:57.072: UDP src=37277, dst=33438
*Dec 29 13:13:57.072: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
```

```
 g=10.1.1.1, len 56, forward
*Dec 29 13:13:57.072: ICMP type=11, code=0
*Dec 29 13:13:57.076: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:13:57.076: UDP src=36884, dst=33439
*Dec 29 13:13:57.076: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 13:13:57.076: ICMP type=11, code=0
```

Essa saída de depuração mostra a sondagem UDP na origem 10.1.1.1 destinada a 10.1.4.2.



Note: Nesses testes, o TTL=2 (não pode ser visto com debug). O dispositivo 11A diminui o TTL para 1 e encaminha os pacotes UDP para o dispositivo 7A. O dispositivo 7A diminui o TTL para zero e responde com mensagens de tempo excedido ICMP.

<#root>

```
*Dec 29 13:13:57.080: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
```

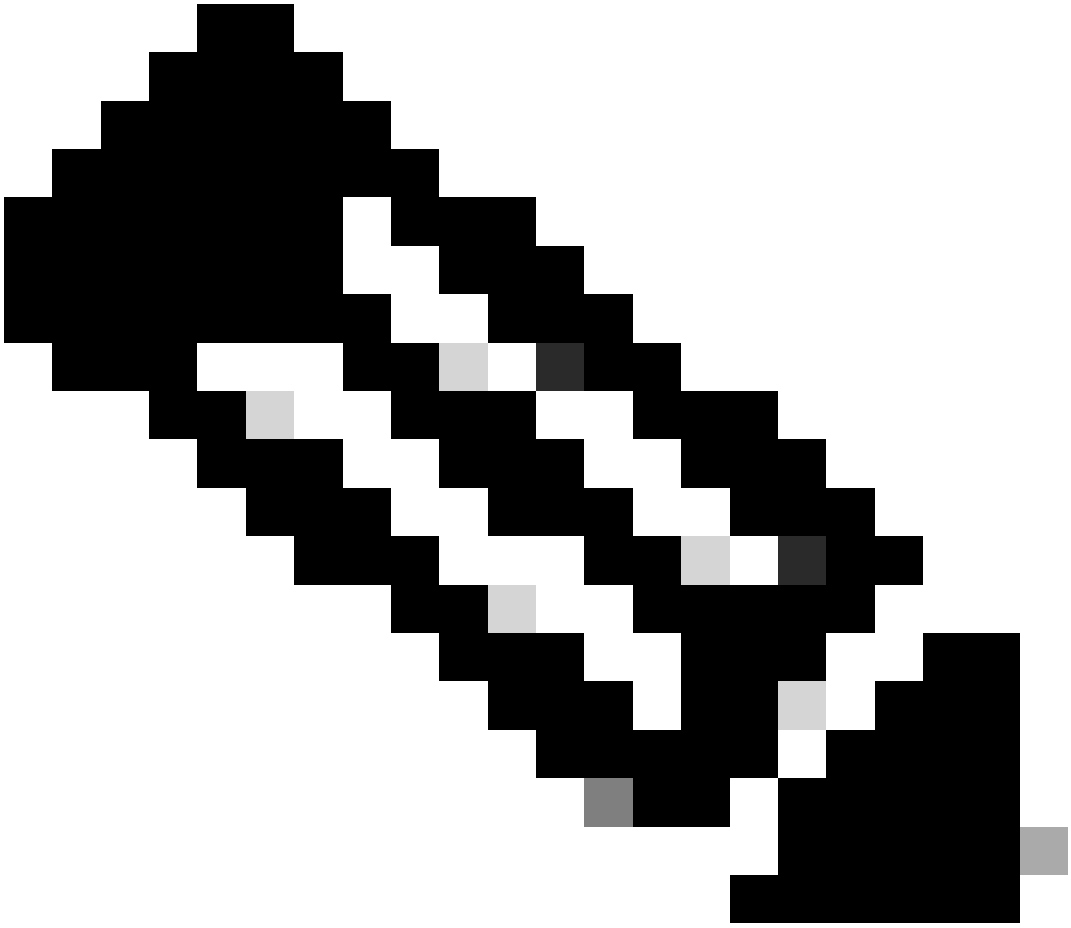
```
*Dec 29 13:13:57.080: UDP src=37479, dst=33440
*Dec 29 13:13:57.080: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 13:13:57.080: ICMP type=11, code=0

*Dec 29 13:13:57.084: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:13:57.084: UDP src=40631, dst=33441
*Dec 29 13:13:57.084: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 13:13:57.084: ICMP type=11, code=0
*Dec 29 13:13:57.084: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:13:57.088: UDP src=39881, dst=33442
*Dec 29 13:13:57.088: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 13:13:57.088: ICMP type=11, code=0
```

As três próximas sondagens UDP são exibidas nessa saída de depuração. O TTL para esses testadores é 3. O dispositivo 11A diminui o TTL para 2 e os encaminha para o dispositivo 7A. O dispositivo 7A diminui o TTL para 1 e encaminha os pacotes para o dispositivo 7B, que diminui o TTL para zero e responde com mensagens de tempo excedido ICMP.

<#root>

```
*Dec 29 13:13:57.088: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:13:57.088: UDP src=39217, dst=33443
*Dec 29 13:13:57.092: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 13:13:57.092: ICMP type=3, code=3

*Dec 29 13:13:57.092: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:13:57.096: UDP src=34357, dst=33444
*Dec 29 13:14:00.092: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:14:00.092: UDP src=39587, dst=33445
*Dec 29 13:14:00.092: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 13:14:00.092: ICMP type=3, code=3
```

Você pode observar as três últimas sondagens UDP nessa saída de depuração. O TTL original desses testadores era 4. O TTL foi diminuído para 3 pelo Dispositivo 11A, em seguida, diminuído para 2 pelo Dispositivo 7A, em seguida, diminuído para 1 pelo Dispositivo 7B. O dispositivo 7C responde com mensagens de porta inalcançável ICMP, já que era o destino das sondas.



Note: O dispositivo 7C envia apenas duas mensagens de porta ICMP inalcançável devido à limitação de taxa.

PC com Linux

<#root>

```
[root#linux-pc]#
```

traceroute -n 10.1.4.2

```
traceroute to 10.1.4.2 (10.1.4.2), 30 hops max, 40 byte packets
1. 10.1.1.2 1.140 ms 0.793 ms 0.778 ms
2. 10.1.2.2 2.213 ms 2.105 ms 3.491 ms
1. 10.1.3.2 3.146 ms 2.314 ms 2.347 ms
1. 10.1.4.2 3.579 ms * 2.954 ms


rp-11a-7204#
```

```
*Jan 2 07:17:27.894: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),
len 56, sending
*Jan 2 07:17:27.894: ICMP type=11, code=0

*Jan 2 07:17:27.894: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),
len 56, sending
*Jan 2 07:17:27.894: ICMP type=11, code=0
*Jan 2 07:17:27.894: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),
len 56, sending
*Jan 2 07:17:27.894: ICMP type=11, code=0
```

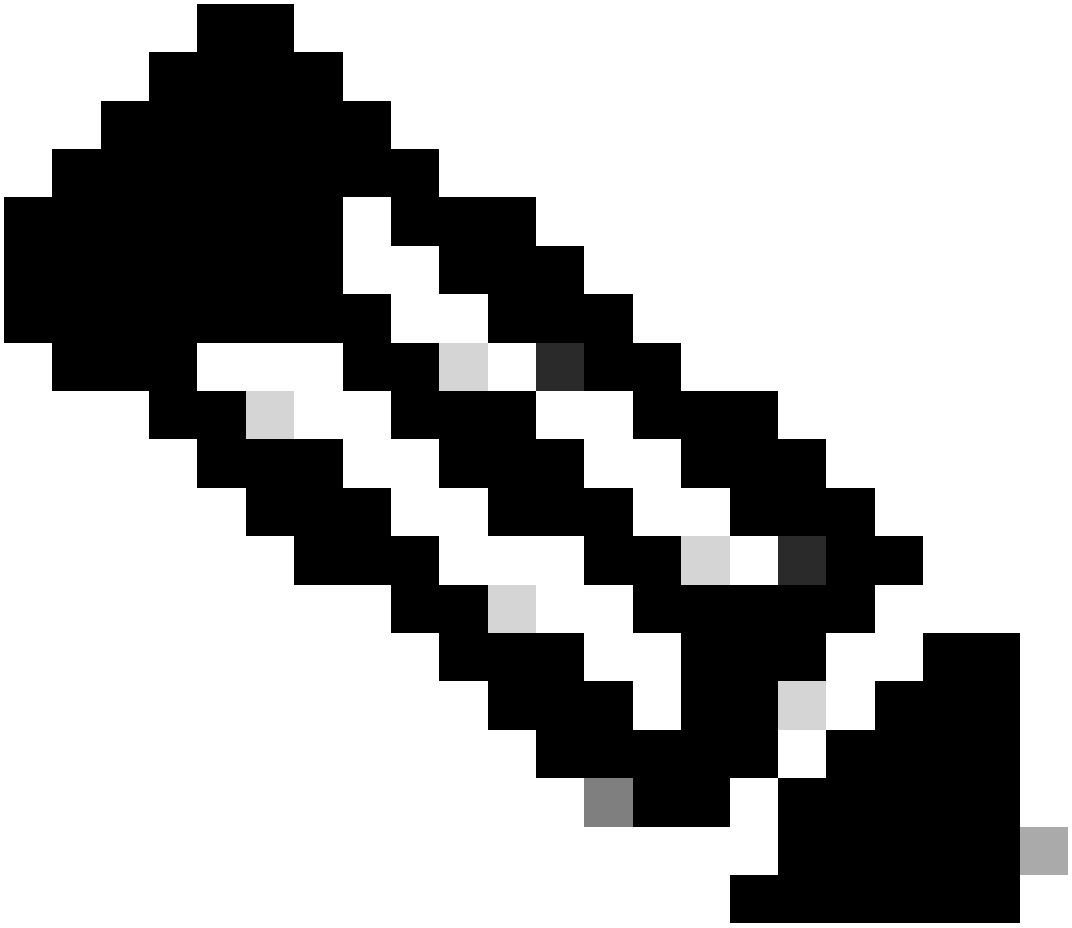
Nesta saída de depuração, o Dispositivo 11A envia mensagens de tempo excedido ICMP à origem dos testadores (10.1.1.1). Essas mensagens ICMP são em resposta às sondas iniciais que tinham um TTL=1. O dispositivo 11A diminui o TTL para zero e responde com as mensagens de tempo excedido.

Você não vê os testes UDP nesta saída de depuração por duas razões:

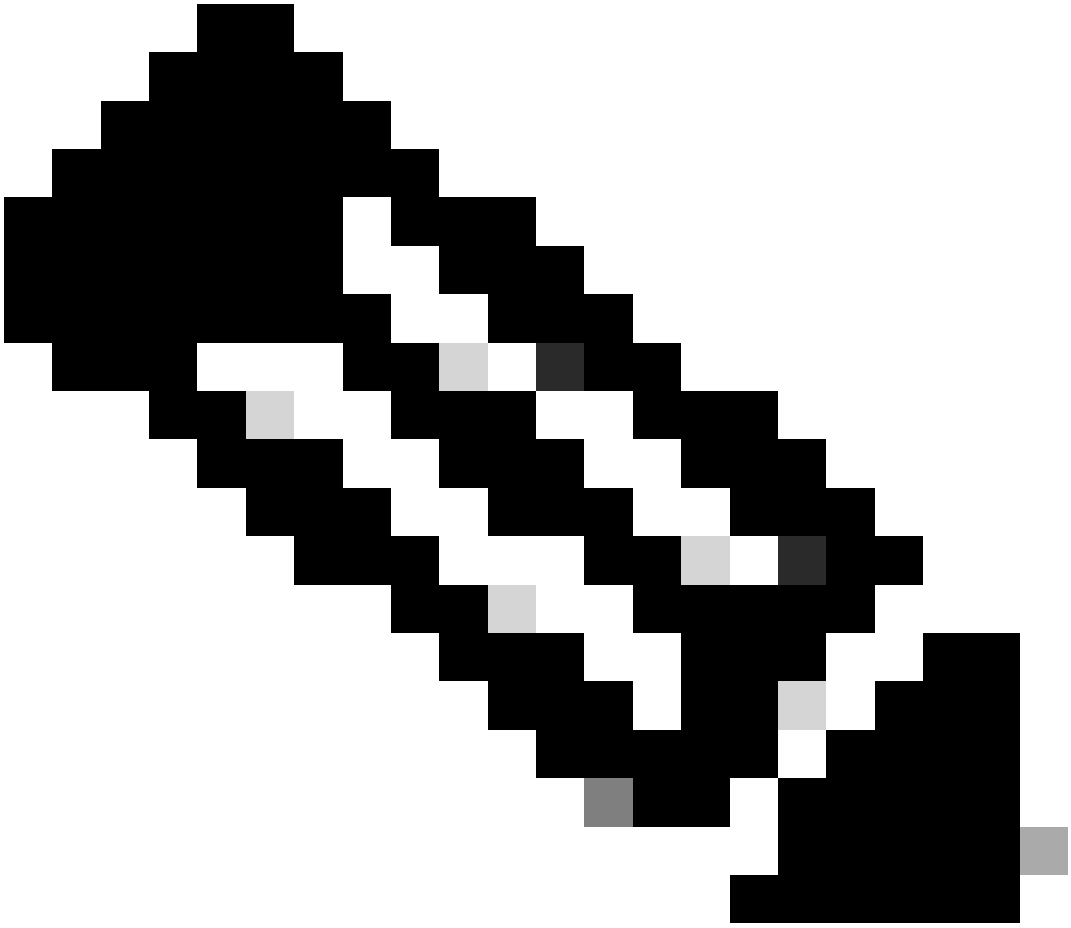
1. O dispositivo 11A não é o destino das sondagens UDP.
2. O TTL é reduzido para zero e o pacote nunca é encaminhado. Portanto, a depuração nunca reconhece o pacote.

<#root>

```
*Jan 2 07:17:27.894: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
*Jan 2 07:17:27.894: UDP src=33302, dst=33438
*Jan 2 07:17:27.898: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1(Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Jan 2 07:17:27.898: ICMP type=11, code=0

*Jan 2 07:17:27.898: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
*Jan 2 07:17:27.898: UDP src=33302, dst=33439
*Jan 2 07:17:27.898: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1(Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Jan 2 07:17:27.898: ICMP type=11, code=0
*Jan 2 07:17:27.898: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
*Jan 2 07:17:27.898: UDP src=33302, dst=33440
*Jan 2 07:17:27.902: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1(Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Jan 2 07:17:27.902: ICMP type=11, code=0
```



Note: Nesta saída de depuração, você agora vê a prova UDP da origem 10.1.1.1 destinada a 10.1.4.2.



Note: Nesses testes, o TTL=2 (não pode ser visto com debug). O dispositivo 11A diminui o TTL para 1 e encaminha os pacotes UDP para o dispositivo 7A. O dispositivo 7A diminui o TTL para zero e responde com mensagens de tempo excedido ICMP.

<#root>

```
*Jan 2 07:17:27.902: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
*Jan 2 07:17:27.902: UDP src=33302, dst=33441
*Jan 2 07:17:27.906: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1(Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Jan 2 07:17:27.906: ICMP type=11, code=0

*Jan 2 07:17:27.906: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
*Jan 2 07:17:27.906: UDP src=33302, dst=33442
*Jan 2 07:17:27.910: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1(Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Jan 2 07:17:27.910: ICMP type=11, code=0
*Jan 2 07:17:27.910: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
```

```
*Jan 2 07:17:27.910: UDP src=33302, dst=33443
*Jan 2 07:17:27.910: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1(Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Jan 2 07:17:27.910: ICMP type=11, code=0
```

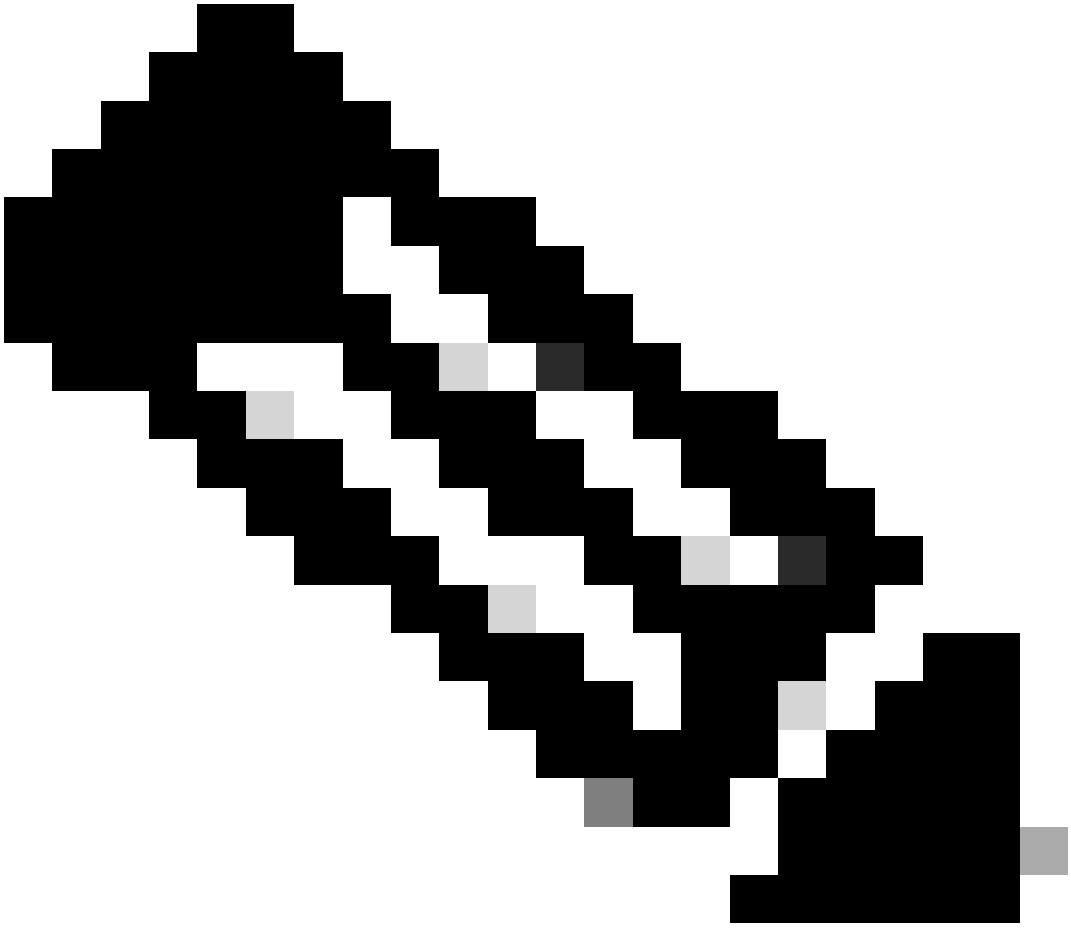
Agora, as três próximas sondagens UDP são exibidas nessa saída de depuração. O TTL para esses testadores é 3. O dispositivo 11A diminui o TTL para 2 e os encaminha para o dispositivo 7A. O dispositivo 7A diminui o TTL para 1 e encaminha os pacotes para o dispositivo 7B, que diminui o TTL para zero e responde com mensagens de tempo excedido ICMP.

<#root>

```
*Jan 2 07:17:27.910: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
*Jan 2 07:17:27.910: UDP src=33302, dst=33444
*Jan 2 07:17:27.914: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1(Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Jan 2 07:17:27.914: ICMP type=3, code=3

*Jan 2 07:17:27.914: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
*Jan 2 07:17:27.914: UDP src=33302, dst=33445
*Jan 2 07:17:32.910: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2(FastEthernet0/0),
 g=10.1.2.2, len 40, forward
*Jan 2 07:17:32.910: UDP src=33302, dst=33446
*Jan 2 07:17:32.914: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1(Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Jan 2 07:17:32.914: ICMP type=3, code=3
```

Essa saída de depuração mostra as três últimas análises UDP. O TTL original desses testadores era 4. O TTL foi diminuído para 3 pelo Dispositivo 11A, em seguida, diminuído para 2 pelo Dispositivo 7A, em seguida, diminuído para 1 pelo Dispositivo 7B.

O Dispositivo 7C responde então com mensagens de porta inalcançável ICMP, já que era o destino das sondas.



Note: O Dispositivo 7C envia apenas duas mensagens ICMP de porta inalcançável devido à limitação de taxa.

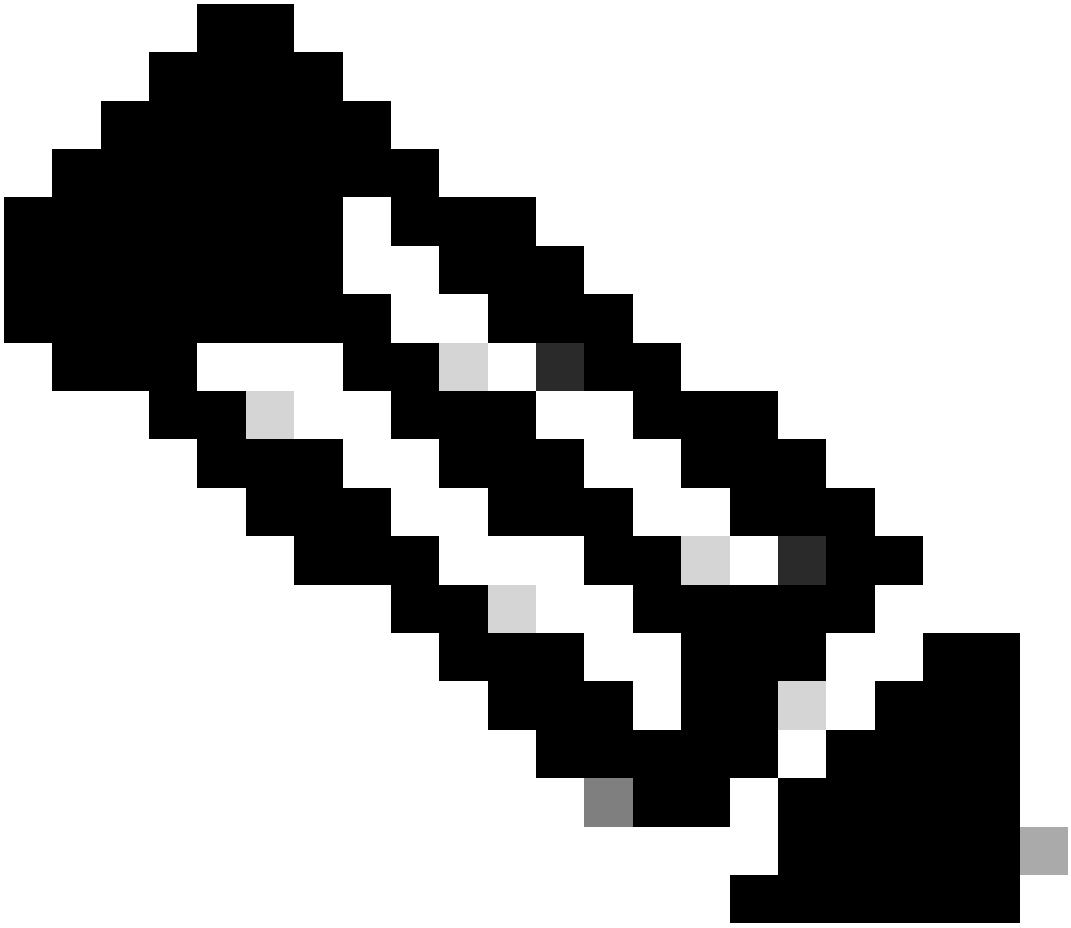
PC executando o MS Windows

<#root>

```
C:\>

tracert 10.1.4.2


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=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 78, forward
*Dec 29 14:02:22.236: UDP src=137, dst=137
*Dec 29 14:02:22.240: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:22.240: ICMP type=3, code=3

*Dec 29 14:02:23.732: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 78, forward
*Dec 29 14:02:23.732: UDP src=137, dst=137
*Dec 29 14:02:23.736: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:23.736: ICMP type=3, code=3
*Dec 29 14:02:25.236: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 78, forward
*Dec 29 14:02:25.236: UDP src=137, dst=137
*Dec 29 14:02:25.236: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:25.240: ICMP type=3, code=3

*Dec 29 14:02:26.748: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),
 len 56, sending
*Dec 29 14:02:26.748: ICMP type=11, code=0

*Dec 29 14:02:26.752: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),
 len 56, sending
*Dec 29 14:02:26.752: ICMP type=11, code=0
*Dec 29 14:02:26.752: IP: s=10.1.1.2 (local), d=10.1.1.1 (Ethernet4/0),
 len 56, sending
*Dec 29 14:02:26.752: ICMP type=11, code=0
```

Nesta saída de depuração, o Dispositivo 11A envia mensagens de tempo excedido ICMP à origem dos testadores (10.1.1.1). Essas mensagens ICMP são em resposta às sondas iniciais, que são pacotes de solicitação de eco ICMP com um TTL=1. O dispositivo 11A diminui o TTL para zero e responde com as mensagens ICMP.



Note: Na parte superior, você verá as solicitações de nome NETBIOS. Essas solicitações são vistas como pacotes UDP com portas origem e destino de 137. Por motivos de clareza, os pacotes NETBIOS são removidos do restante da saída de depuração. Você pode usar a **-d** opção no comando para desativar o comportamento do NETBIOS **tracert** .

Você não vê os testes ICMP nesta saída de depuração por duas razões:

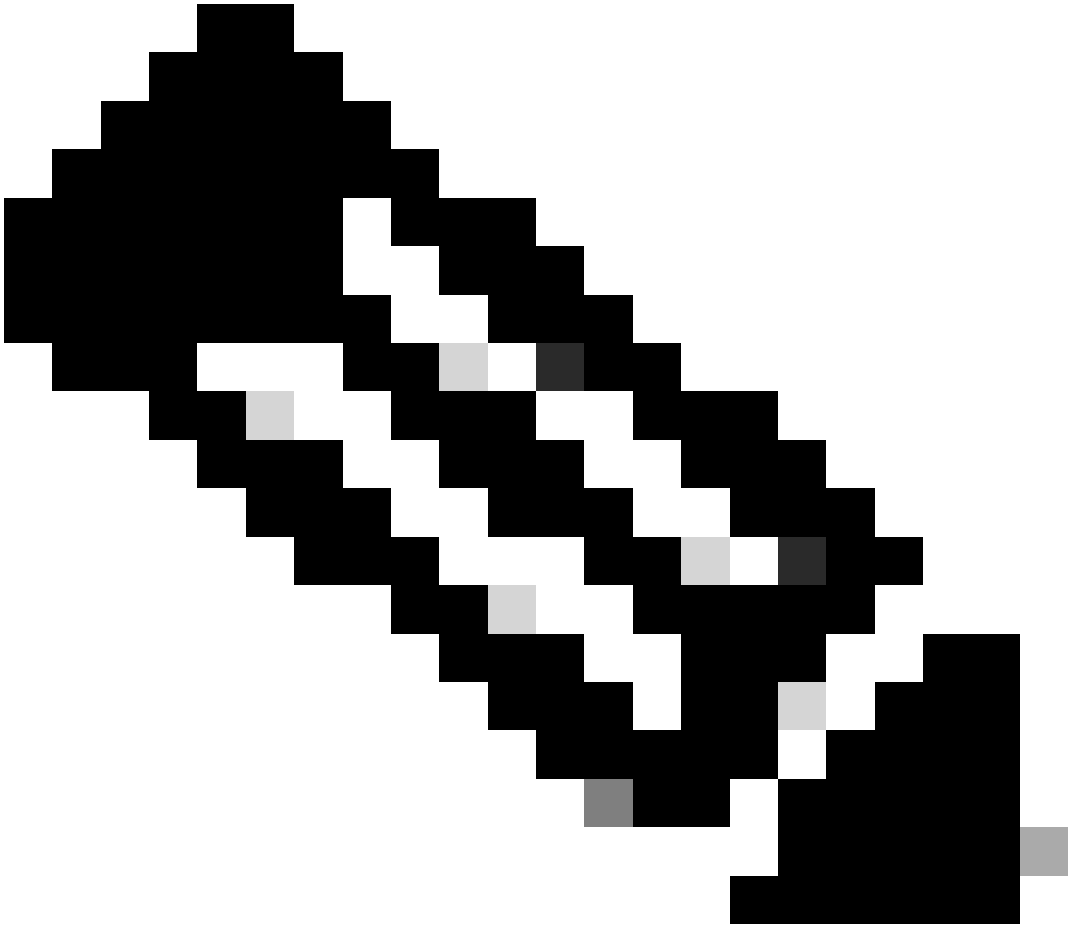
1. O dispositivo 11A não é o destino das sondagens ICMP.
2. O TTL é reduzido para zero e o pacote nunca é encaminhado. Portanto, a depuração nunca reconhece o pacote.

<#root>

```
*Dec 29 14:02:32.256: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:32.256: ICMP type=8, code=0
```

```
*Dec 29 14:02:32.260: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:32.260: ICMP type=11, code=0

*Dec 29 14:02:32.260: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:32.260: ICMP type=8, code=0
*Dec 29 14:02:32.260: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:32.260: ICMP type=11, code=0
*Dec 29 14:02:32.264: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:32.264: ICMP type=8, code=0
*Dec 29 14:02:32.264: IP: s=10.1.2.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:32.264: ICMP type=11, code=0
```

Nessa saída de depuração, agora a sondagem ICMP é exibida na origem 10.1.1.1 destinada a 10.1.4.2.



Note: Nesses testes, o TTL=2 (isso não pode ser visto com debug). O dispositivo 11A

---

diminui o TTL para 1 e encaminha os pacotes UDP para o dispositivo 7A. O dispositivo 7A diminui o TTL para zero e responde com mensagens de tempo excedido ICMP.

<#root>

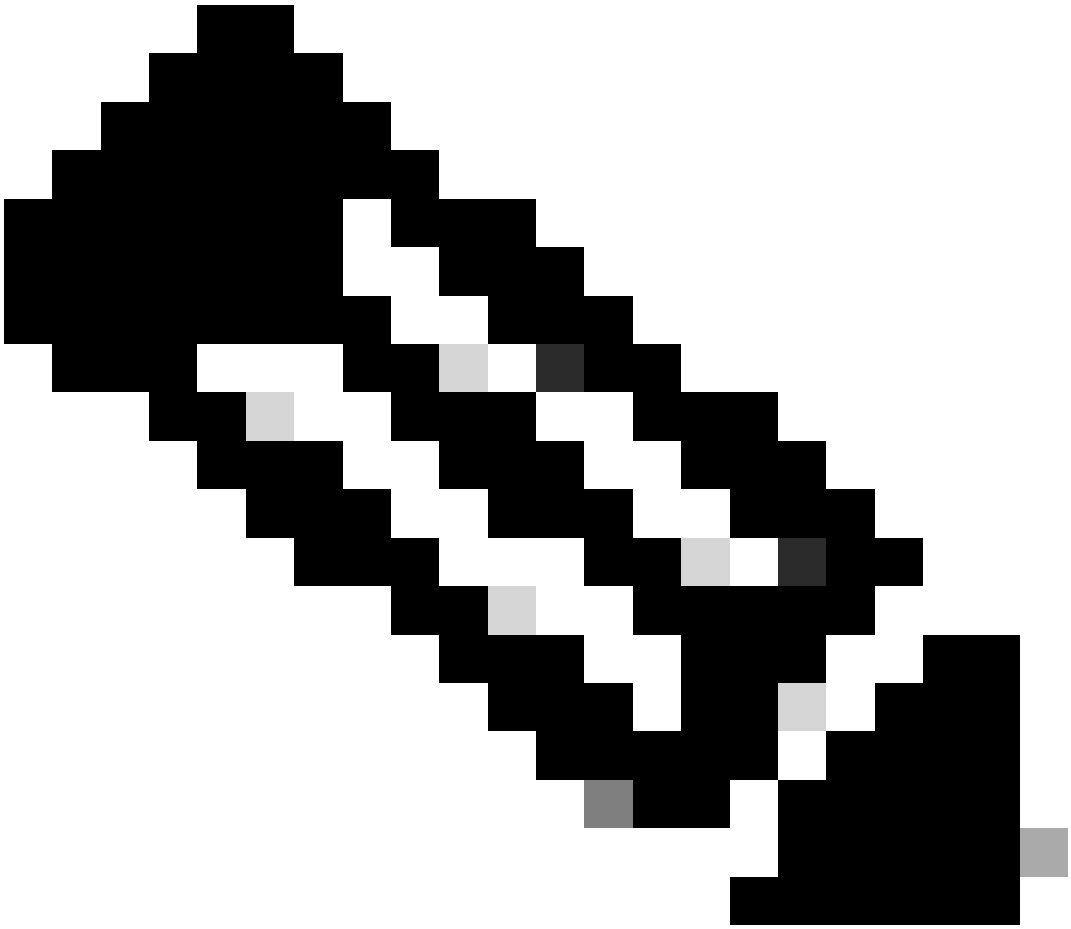
```
*Dec 29 14:02:37.776: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:37.776: ICMP type=8, code=0
*Dec 29 14:02:37.776: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:37.776: ICMP type=11, code=0

*Dec 29 14:02:37.780: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:37.780: ICMP type=8, code=0
*Dec 29 14:02:37.780: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:37.780: ICMP type=11, code=0
*Dec 29 14:02:37.780: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:37.780: ICMP type=8, code=0
*Dec 29 14:02:37.784: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:37.784: ICMP type=11, code=0
```

As três próximas sondagens ICMP são exibidas nessa saída de depuração. O TTL para esses testadores é 3. O dispositivo 11A diminui o TTL para 2 e os encaminha para o dispositivo 7A. O dispositivo 7A diminui o TTL para 1 e encaminha os pacotes para o dispositivo 7B, que diminui o TTL para zero e responde com mensagens de tempo excedido ICMP.

<#root>

```
*Dec 29 14:02:43.292: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:43.292: ICMP type=8, code=0
*Dec 29 14:02:43.296: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 92, forward
*Dec 29 14:02:43.296: ICMP type=0, code=0

*Dec 29 14:02:43.296: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:43.296: ICMP type=8, code=0
*Dec 29 14:02:43.300: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 92, forward
*Dec 29 14:02:43.300: ICMP type=0, code=0
*Dec 29 14:02:43.300: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:43.300: ICMP type=8, code=0
*Dec 29 14:02:43.304: IP: s=10.1.4.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 92, forward
*Dec 29 14:02:43.304: ICMP type=0, code=0
```

Esta saída de depuração mostra as três últimas análises UDP. O TTL original desses testadores era 4. O TTL foi diminuído para 3 pelo Dispositivo 11A, em seguida, diminuído para 2 pelo Dispositivo 7A, em seguida, diminuído para 1 pelo Dispositivo 7B. O dispositivo 7C responde com mensagens de resposta de eco do ICMP (tipo=0, código=0), pois era o destino das sondagens.



> Note: As mensagens de resposta de eco ICMP não têm taxa limitada, como as mensagens de porta inalcançável ICMP. Nesse caso, são exibidas todas as três mensagens de resposta de eco do ICMP enviadas.

Notas adicionais

Nos roteadores Cisco, os códigos para uma `traceroute` resposta de comando são:

```
! -- 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)
```

Se você executar o comando traceroute a partir do UNIX, observe estes itens:

- Você pode receber traceroute: icmp socket: Permission denied mensagens.
- O programa traceroute conta com o Network Interface Tap (NIT) para rastrear a rede. Este dispositivo só pode ser acessado pelo root. Você deve executar o programa como root ou definir a ID do usuário para root.

Summary

Este documento demonstrou como o comando traceroute determina o caminho que um pacote percorre de uma determinada origem para um determinado destino com o uso de pacotes UDP e ICMP. Os tipos possíveis de mensagens do ICMP nas saídas são:

- Se o TTL for excedido em trânsito, tipo=11, código=0, o pacote será devolvido pelo roteador de trânsito em todos os casos em que o TTL dos pacotes de sondagem expirar antes que os pacotes cheguem ao destino.
- Se a porta estiver inacessível, tipo=3, código=3, o pacote será devolvido em resposta aos pacotes de sondagem UDP, quando chegarem ao destino (a aplicação UDP não foi definida). Esses pacotes são limitados a um pacote por 500 ms. Isso explica por que a resposta do destino (consulte as saídas do roteador Cisco e do Linux) falhou nas respostas pares. O dispositivo 7C não gera a mensagem ICMP e a saída do traceroute comando em cada dispositivo aguarda por mais de um segundo. No caso da saída do comando MS Windows tracert , a mensagem ICMP é gerada porque a porta UDP 137 não existe em um roteador Cisco.
- Se houver um eco, tipo=8, código=0, o pacote de sondagem de eco será enviado pelo PC com MS Windows.
- Se houver uma resposta de eco, tipo=0, código=0, uma resposta ao pacote anterior será enviada quando o destino for alcançado. Isso se aplica somente ao comando MS Windows tracert .

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.