Uso del comando traceroute nei vari sistemi operativi

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati
- Convenzioni

Premesse

Funzionamento generale

- Cisco IOS e Linux
- Microsoft Windows

Limitazione della velocità degli elementi non raggiungibili ICMP

Esempi

- Router Cisco con software Cisco IOS
- PC con Linux
- PC con MS Windows

Note aggiuntive

Riepilogo

Informazioni correlate

Introduzione

In questo documento viene descritto il funzionamento del `traceroute` comando su diversi sistemi.

Prerequisiti

Requisiti

I lettori di questo documento devono avere una conoscenza di base di uno dei seguenti sistemi operativi:

- Software Cisco IOS®
- Linux
- Microsoft Windows

Componenti usati

Le informazioni di questo documento si applicano alle seguenti versioni software e hardware:

- Router Cisco con software Cisco IOS versione 12
- PC con Red Hat Linux
- PC con MS Windows

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Il comando traceroute permette di determinare il percorso di un pacchetto per raggiungere una destinazione da una determinata origine, restituendo la sequenza di hop attraversati dal pacchetto. Questa utility viene fornita con il sistema operativo host (ad esempio, Linux o Microsoft (MS) Windows), nonché con il software Cisco IOS.

Funzionamento generale

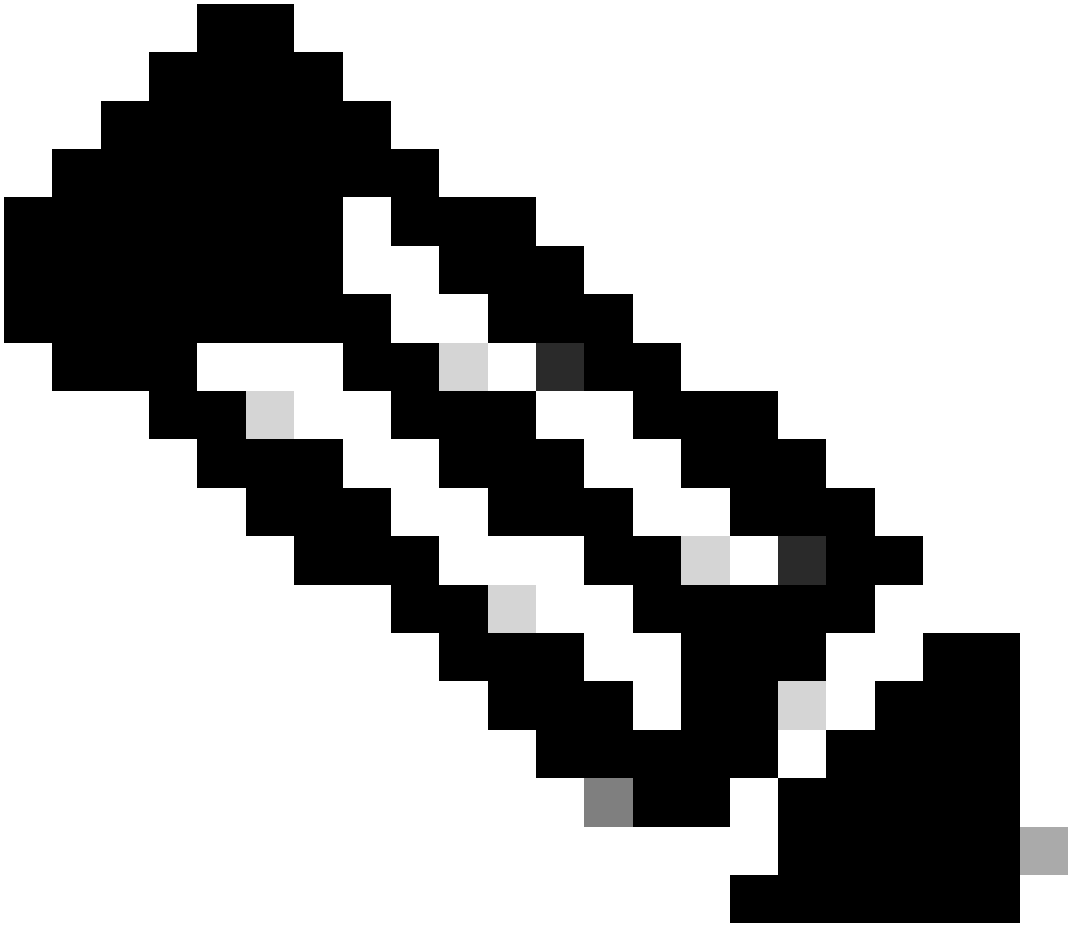
Se si esegue il comando traceroute ip-address su un dispositivo di origine (ad esempio un host o un router che opera come host), i pacchetti IP vengono inviati alla destinazione con valori TTL (Time To Live) incrementabili fino al numero massimo di hop specificato. Per impostazione predefinita, questo valore è 30. In genere, ciascun router del percorso verso la destinazione diminuisce il campo TTL di un'unità mentre inoltra i pacchetti. Quando un router al centro del percorso trova un pacchetto con TTL = 1, risponde all'origine con un messaggio ICMP (Internet Control Message Protocol) "tempo scaduto". Questo messaggio comunica all'origine che il pacchetto attraversa quel particolare router come hop

Ci sono alcune differenze con il modo in cui il comando traceroute è implementato nei vari sistemi operativi discussi in questo documento.

Cisco IOS e Linux

Il valore TTL della sonda del datagramma UDP (User Datagram Protocol) iniziale è impostato su 1 (o sul valore TTL minimo, come specificato dall'utente nel traceroute comando esteso). La porta UDP di destinazione della sonda del datagramma iniziale è impostata su 33434 (o come specificato nell'output del traceroute comando esteso). Il comando esteso traceroute è una variante del comando ordinario traceroute traceroute che consente di modificare i valori predefiniti dei parametri utilizzati dall'operazione, ad esempio TTL e numero di porta di destinazione. Per ulteriori informazioni su

come usare il traceroute comando esteso, consultare il documento sulla descrizione dei comandi ping esteso e traceroute esteso. La porta UDP di origine della sonda del datagramma iniziale è casuale e dispone di un operatore logico OR con 0x8000 (garantisce una porta di origine minima di 0x8000). Di seguito viene descritto cosa succede quando viene avviato il datagramma UDP:



Nota: I parametri sono configurabili. Questo esempio inizia con n = 1 e finisce con n = 3.

---

1. Il datagramma UDP viene inviato con TTL = 1, la porta UDP di destinazione = 33434 e la porta di origine casualmente.
2. La porta di destinazione UDP viene incrementata, la porta UDP di origine viene assegnata in modo casuale e il secondo datagramma viene inviato.
3. Il passaggio 2 viene ripetuto per un massimo di tre richieste (o per tutte le volte richieste in un output del traceroute comando esteso). Per ognuna delle richieste inviate, viene visualizzato un messaggio "TTL superato", che viene utilizzato per creare un percorso dettagliato all'host di destinazione.

4. Il valore TTL viene incrementato e il ciclo viene ripetuto con i numeri delle porte di destinazione incrementali, se viene ricevuto il messaggio ICMP "tempo scaduto". È inoltre possibile ricevere uno dei messaggi seguenti:

    - Un messaggio ICMP tipo 3, codice 3 (destinazione irraggiungibile, porta non raggiungibile), che indica che è stato raggiunto un host.
    - È stato superato il valore TTL massimo per un host non raggiungibile, net non raggiungibile o un tipo di timeout del messaggio, ossia la sonda è stata inviata di nuovo.

I router Cisco inviano pacchetti di sonde UDP con una porta di origine casuale e una porta di destinazione incrementale (per distinguere le diverse sonde). I router Cisco restituiscono il tempo scaduto per i messaggi ICMP all'origine dal quale il pacchetto UDP/ICMP è stato ricevuto.

Il comando Linux `traceroute` è simile al router Cisco. Tuttavia, utilizza una porta di origine fissa. L'opzione `-n` nel `traceroute` comando viene utilizzata per evitare una richiesta a un server dei nomi.

Microsoft Windows

Il`tracert`comando MS Windows utilizza i datagrammi di richiesta echo ICMP anziché i datagrammi UDP come sonde. Le richieste echo ICMP vengono avviate con un TTL incrementale e si verifica la stessa operazione descritta in Cisco IOS e Linux. Il significato dell'uso dei datagrammi ICMP di richiesta echo è che l'hop finale non si basa sulla risposta di un messaggio ICMP "destinazione irraggiungibile" dall'host di destinazione. Si basa invece su un messaggio di risposta echo ICMP.

La sintassi del comando è:

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

In questa tabella vengono descritti i parametri del comando:

Parametro	Descrizione
-d	Specifica di non risolvere gli indirizzi nei nomi dei computer.
-h numero_massimo_hop	Specifica il numero massimo di hop per la ricerca di una destinazione.
-j elenco-computer	Specifica una route di origine libera lungo l'elenco dei computer.
-w timeout	Attende il numero di millisecondi specificato dal timeout per ogni risposta.
nome_destinazione	Nome del computer di destinazione.

Limitazione della velocità degli elementi non raggiungibili ICMP

Gli elementi non raggiungibili ICMP sono limitati a un pacchetto per 500 ms (come protezione da

attacchi Denial of Service (DoS)) in un router Cisco. Dal software Cisco IOS versione 12.1 e successive, questo valore di velocità è configurabile. Il comando introdotto è:

<#root>

Router(config)#

```
ip icmp rate-limit unreachable ?

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

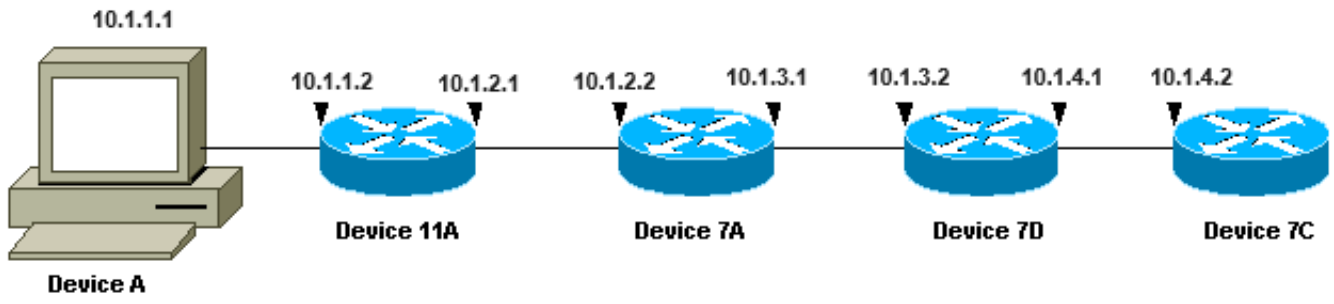
Come mostrato nell'output, questa limitazione si riferisce alla velocità aggregata di tutti gli elementi ICMP non raggiungibili. Per ulteriori informazioni, fare riferimento alla RFC 792.

```
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.
```

Questa limitazione non influenza altri pacchetti come le richieste echo ICMP o i messaggi ICMP "time exceeded" (tempo scaduto).

Esempi

Questa topologia di rete viene utilizzata per gli esempi seguenti:



Topologia della rete

In ognuno dei tre esempi viene utilizzato un dispositivo A diverso. Dal dispositivo A, il comando traceroute 10.1.4.2 viene eseguito sul dispositivo 7C.

In ciascuno degli esempi, il comando debug ip packet detail viene eseguito sul dispositivo 11A.

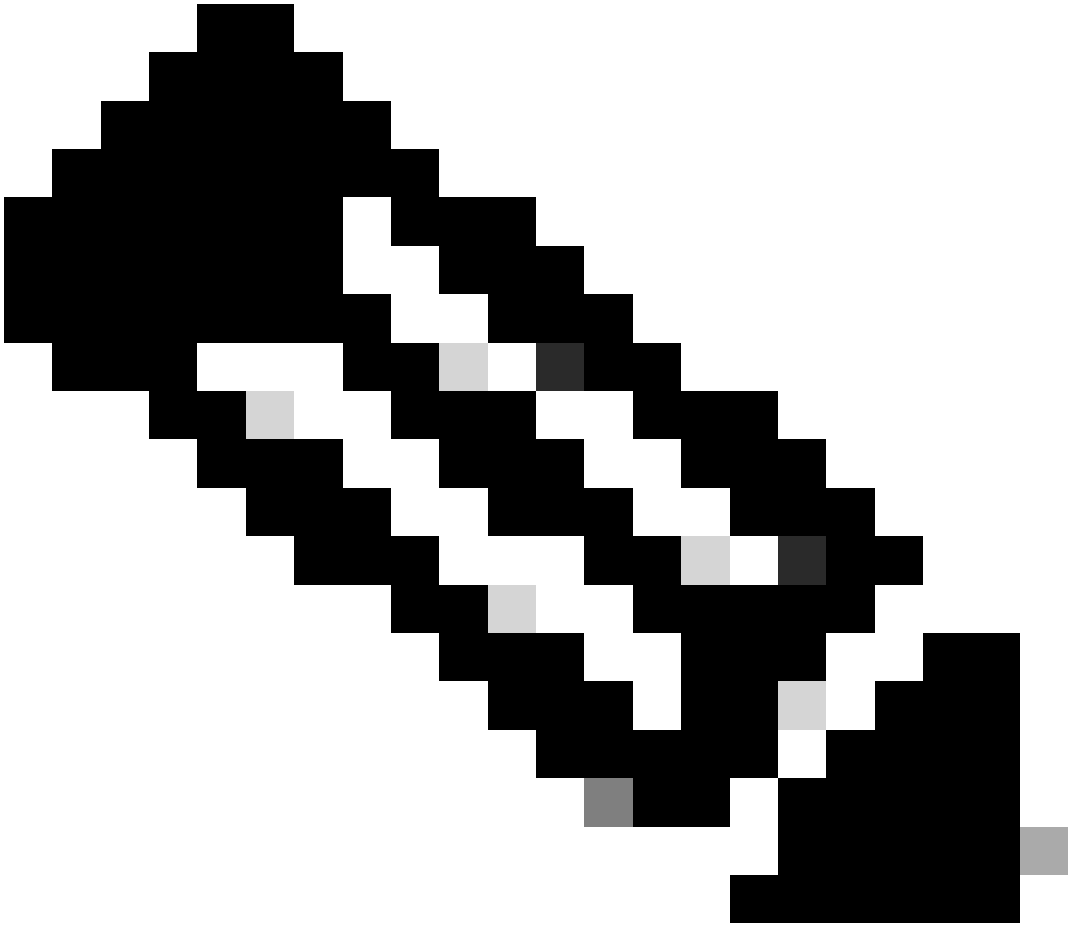
Router Cisco con software Cisco IOS

Nell'esempio di traceroute comando esteso vengono mostrate le opzioni che è possibile modificare quando si esegue un traceroute comando da un router Cisco. In questo esempio, vengono mantenute le impostazioni predefinite:

<#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
```

In questo output di debug, il dispositivo 11A invia messaggi ICMP "tempo scaduto" all'origine delle sonde (10.1.1.1). Questi messaggi ICMP sono in risposta alle richieste iniziali che avevano un TTL=1. Il dispositivo 11A riduce il TTL a zero e risponde con i messaggi di tempo scaduto.



Nota: Le richieste UDP non vengono visualizzate in questo output di debug per due motivi:

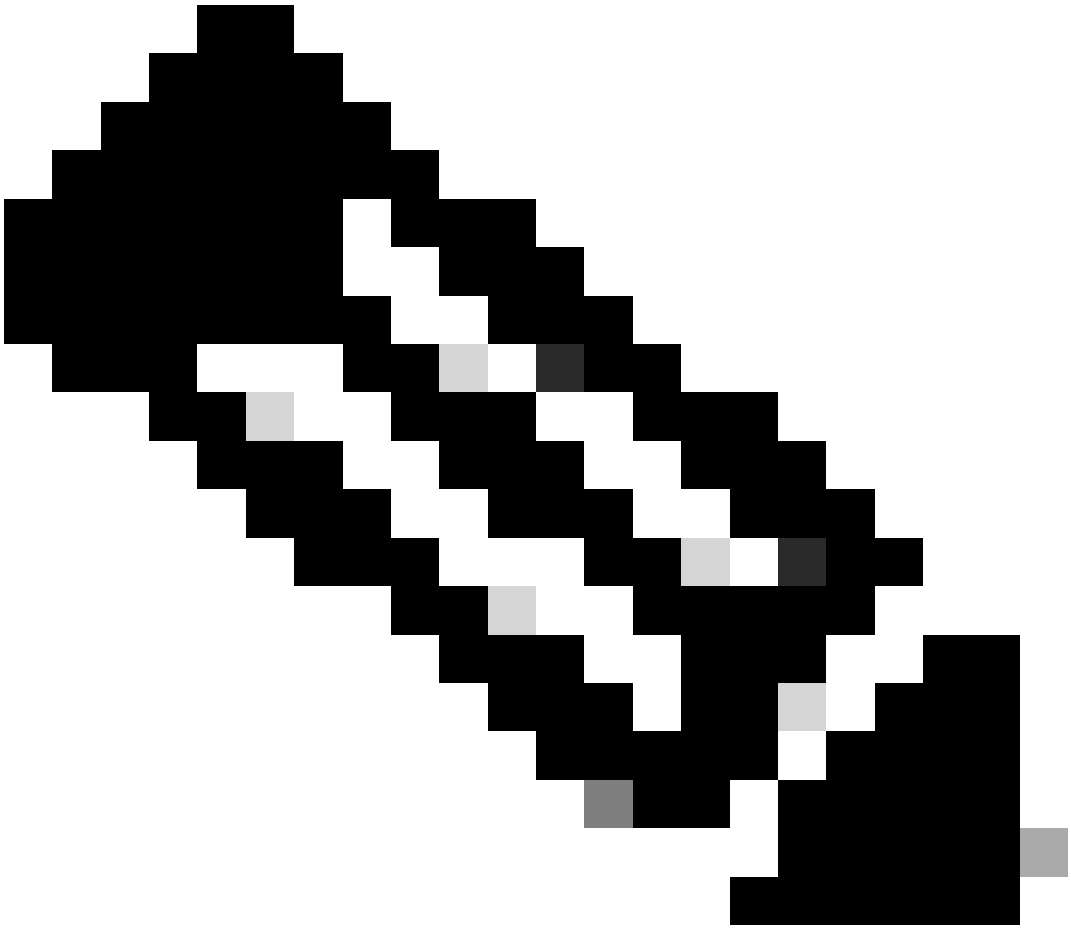
- La periferica 11A non è la destinazione delle sonde UDP.
- Il valore TTL viene ridotto a zero e il pacchetto non viene mai indirizzato. Pertanto, il debug non riconosce mai il pacchetto.

<#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
```

Questo output di debug visualizza la sonda UDP dall'origine 10.1.1.1 destinata a 10.1.4.2.



Nota: In queste richieste, TTL=2 (non visualizzabile con debug). Il dispositivo 11A riduce il valore TTL a 1 e inoltra i pacchetti UDP sul dispositivo 7A. Il dispositivo 7A azzera il valore TTL e risponde con i messaggi ICMP "time exceeded" (tempo scaduto).

<#root>

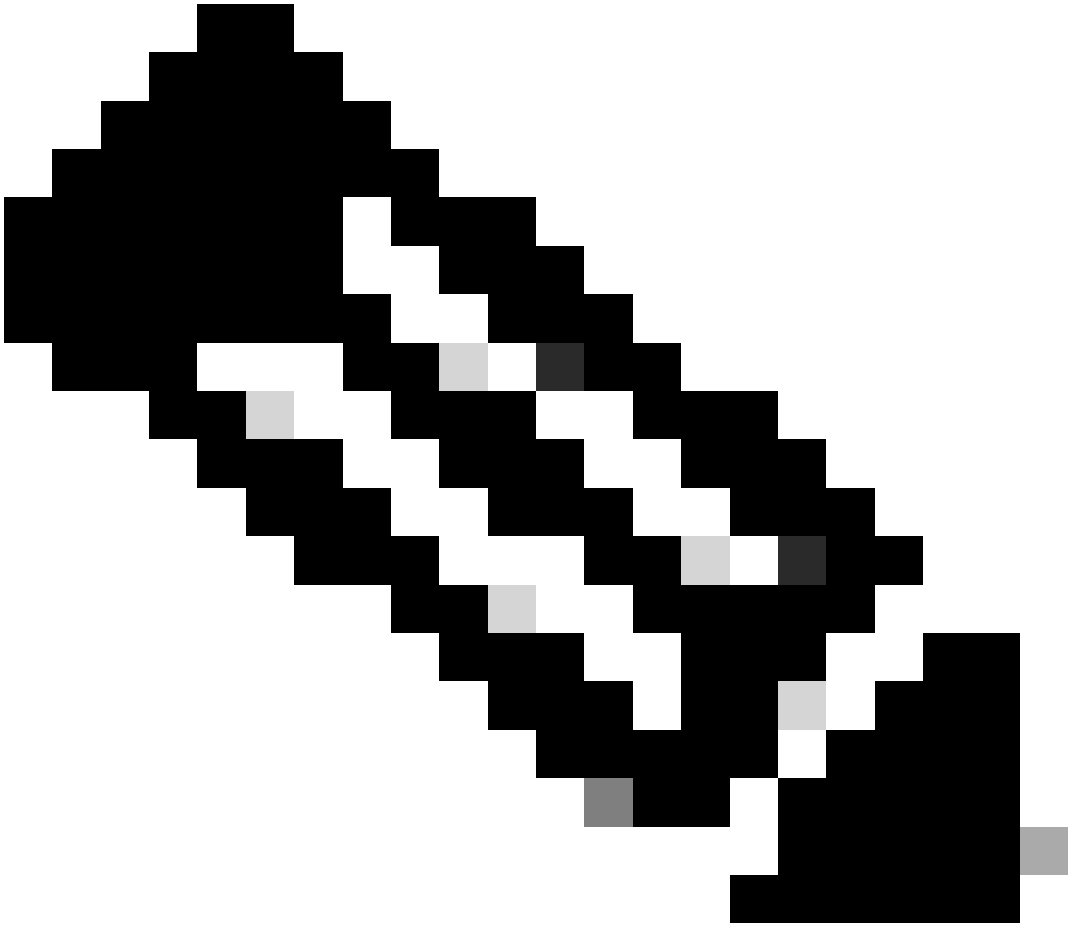
```
*Dec 29 13:13:57.080: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 28, forward
*Dec 29 13:13:57.080: UDP src=37479, dst=33440
*Dec 29 13:13:57.080: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 13:13:57.080: ICMP type=11, 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
```

In questo output del comando debug, vengono visualizzate le tre richieste UDP successive. Il valore TTL di queste sonde è 3. Il dispositivo 11A riduce il valore TTL a 2 e lo inoltra al dispositivo 7A. Il dispositivo 7A riduce il valore TTL a 1 e inoltra i pacchetti al dispositivo 7B, che riduce il valore TTL a zero e risponde con i messaggi ICMP "tempo scaduto".

<#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
```

In questo output di debug, è possibile visualizzare le ultime tre richieste UDP. Il valore TTL originale di queste sonde era 4. Il valore TTL è stato diminuito a 3 dal dispositivo 11A, quindi è stato diminuito a 2 dal dispositivo 7A, infine è stato diminuito a 1 dal dispositivo 7B. Il dispositivo 7C risponde con messaggi ICMP "port unreachable" (porta non raggiungibile) perché era la destinazione delle sonde.



Nota: Il dispositivo 7C invia solo due messaggi ICMP "destinazione irraggiungibile" a causa del limite di velocità.

PC con 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
```

In questo output di debug, il dispositivo 11A invia messaggi ICMP "tempo scaduto" all'origine delle sonde (10.1.1.1). Questi messaggi ICMP sono in risposta alle richieste iniziali che avevano un TTL=1. Il dispositivo 11A riduce il TTL a zero e risponde con i messaggi di tempo scaduto.

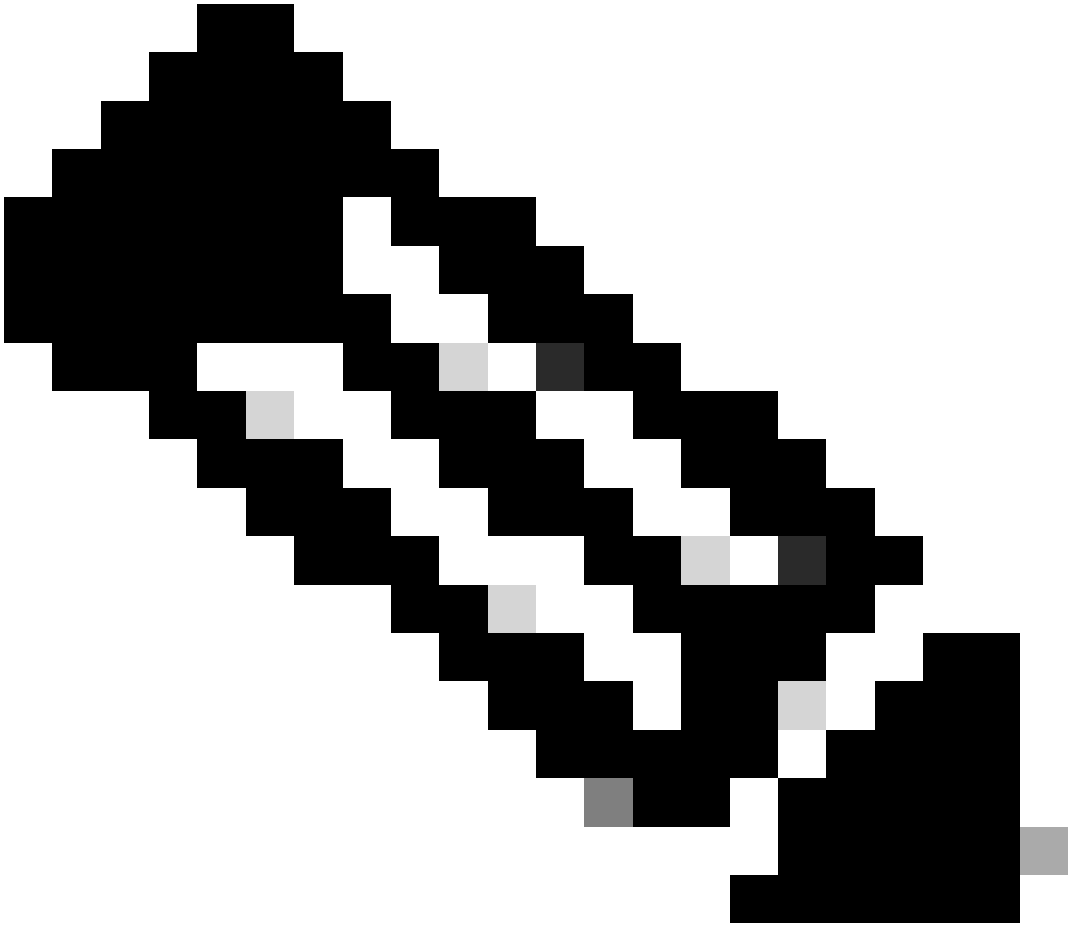
Le richieste UDP non vengono visualizzate in questo output di debug per due motivi:

1. La periferica 11A non è la destinazione delle sonde UDP.
2. Il valore TTL viene ridotto a zero e il pacchetto non viene mai indirizzato. Pertanto, il debug non riconosce mai il pacchetto.

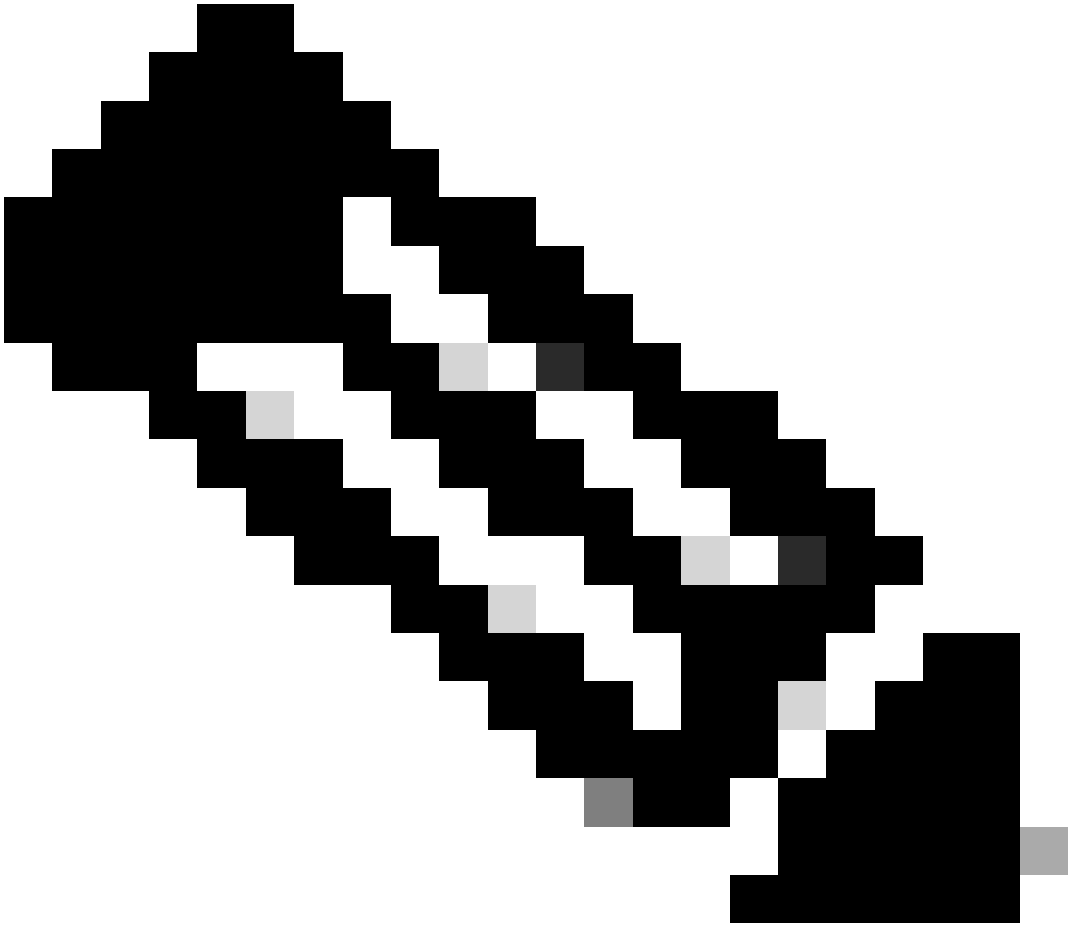
<#root>

```
*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
```



Nota: In questo output del comando debug, è ora possibile vedere la sonda UDP dall'origine 10.1.1.1 destinata alla versione 10.1.4.2.



Nota: In queste richieste, TTL=2 (non visualizzabile con debug). Il dispositivo 11A riduce il valore TTL a 1 e inoltra i pacchetti UDP sul dispositivo 7A. Il dispositivo 7A azzera il valore TTL e risponde con i messaggi ICMP "time exceeded" (tempo scaduto).

<#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
```

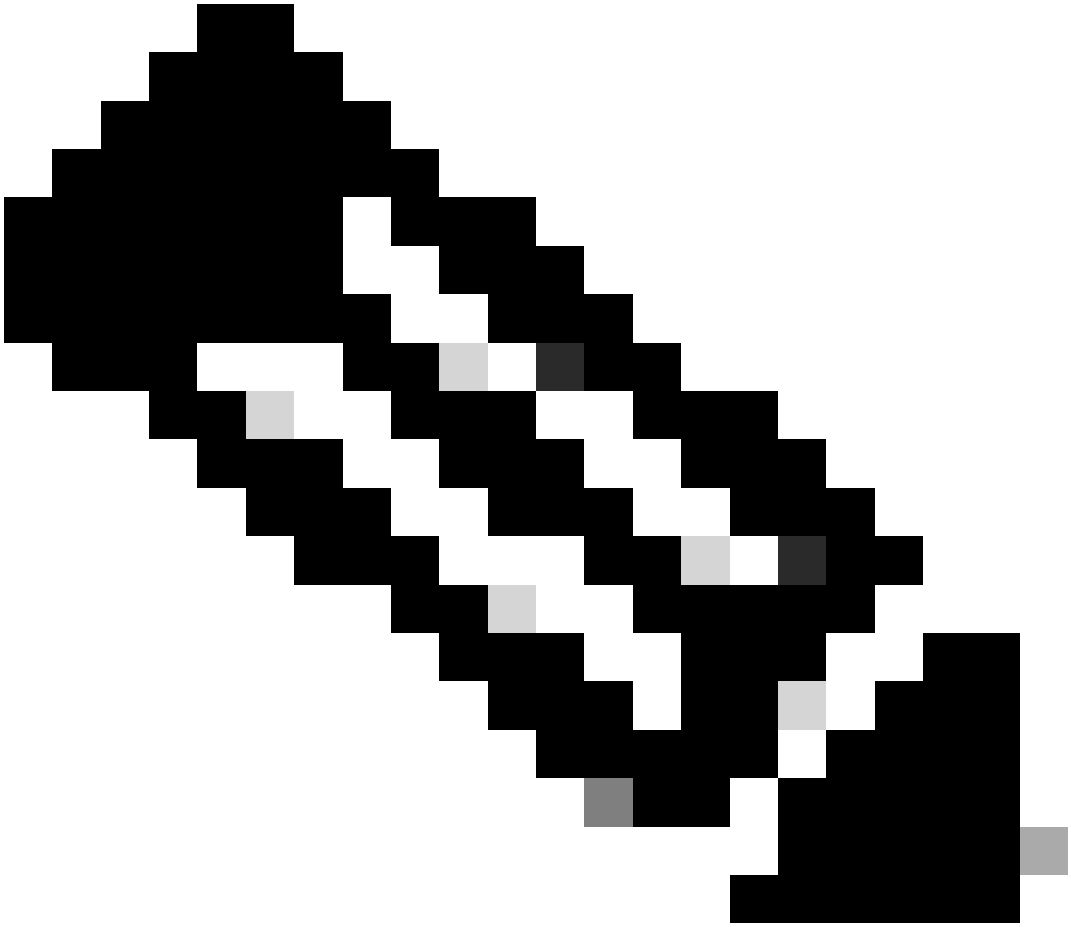
Le tre richieste UDP successive sono ora visualizzate in questo output di debug. Il valore TTL di queste sonde è 3. Il dispositivo 11A riduce il valore TTL a 2 e lo inoltra al dispositivo 7A. Il dispositivo 7A riduce il valore TTL a 1 e inoltra i pacchetti al dispositivo 7B, che riduce il valore TTL a zero e risponde con i messaggi ICMP "tempo scaduto".

<#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
```

Questo output di debug visualizza le ultime tre richieste UDP. Il valore TTL originale di queste sonde era 4. Il valore TTL è stato diminuito a 3 dal dispositivo 11A, quindi è stato diminuito a 2 dal dispositivo 7A, infine è stato diminuito a 1 dal dispositivo 7B.

Il dispositivo 7C risponde quindi con messaggi ICMP "port unreachable" (porta non raggiungibile), in quanto era la destinazione delle sonde.



Nota: Il dispositivo 7C invia solo due messaggi ICMP "destinazione irraggiungibile" a causa della limitazione della velocità.

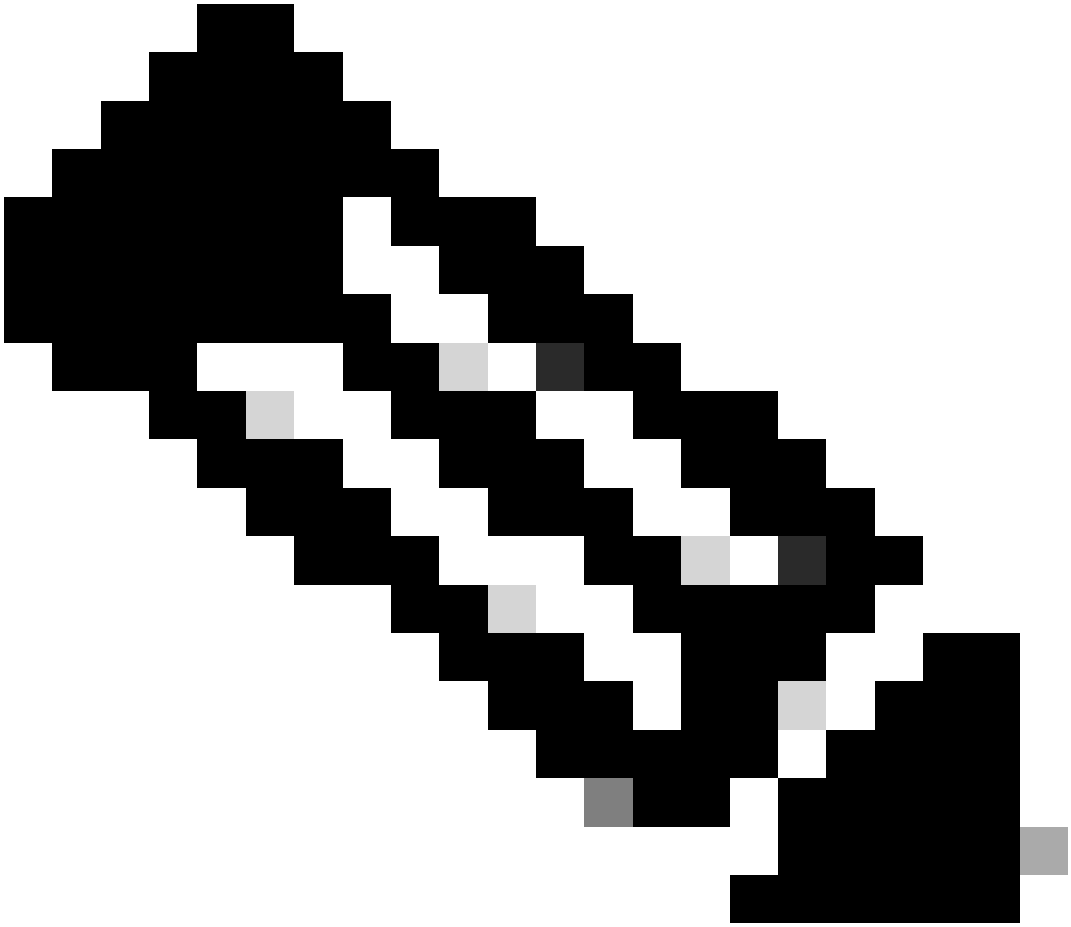
PC con MS Windows

<#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
```

In questo output di debug, il dispositivo 11A invia messaggi ICMP "tempo scaduto" all'origine delle sonde (10.1.1.1). Questi messaggi ICMP sono in risposta alle richieste iniziali, ossia pacchetti di richieste echo ICMP con TTL=1. Il dispositivo 11A riduce il valore TTL a zero e risponde con i messaggi ICMP.



Nota: Nella parte superiore vengono visualizzate le richieste di nomi NETBIOS. Queste richieste vengono considerate come pacchetti UDP con porte di origine e di destinazione pari a 137. Per motivi di chiarezza, i pacchetti NETBIOS vengono rimossi dal resto dell'output di debug. È possibile utilizzare l' **-d** opzione nel **tracert** comando per disattivare il comportamento NETBIOS.

Le richieste ICMP non vengono visualizzate in questo output di debug per due motivi:

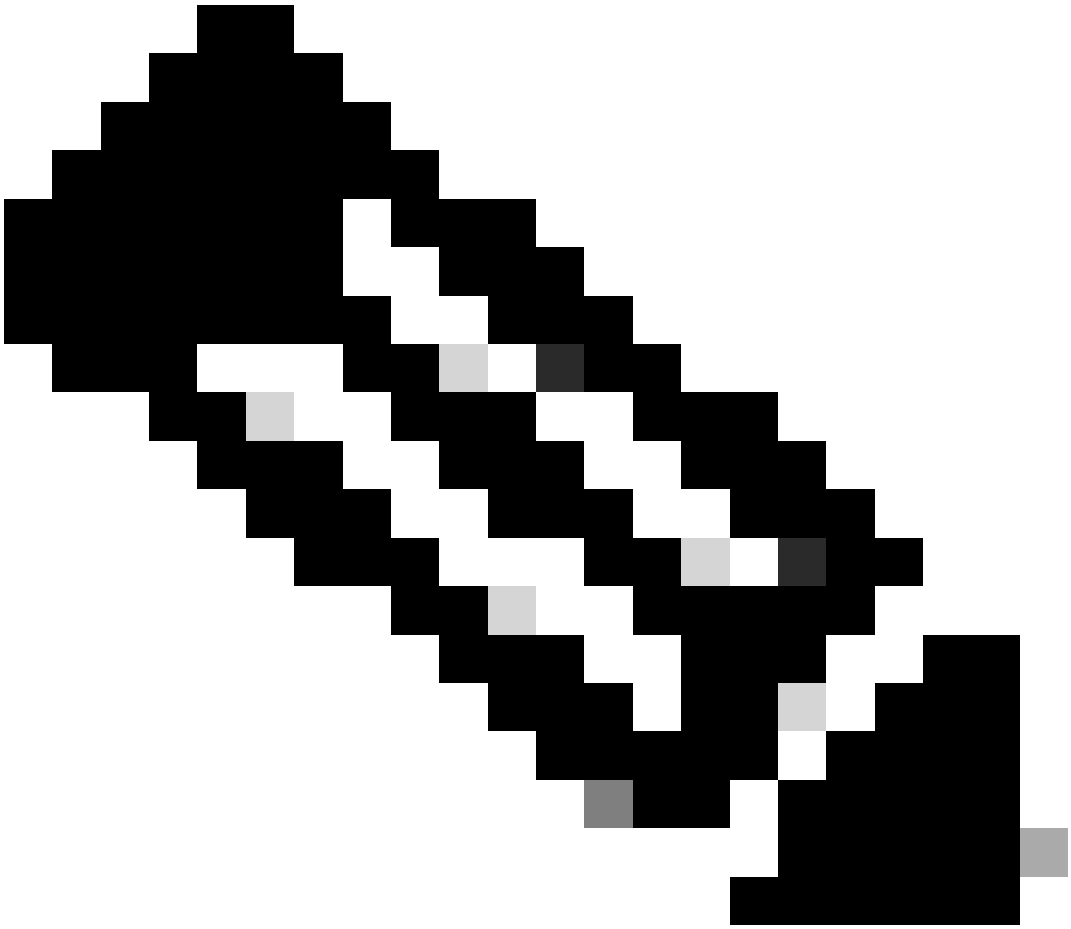
1. La periferica 11A non è la destinazione delle sonde ICMP.
2. Il valore TTL viene ridotto a zero e il pacchetto non viene mai indirizzato. Pertanto, il debug non riconosce mai il pacchetto.

<#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
```

In questo output di debug, è ora possibile vedere la sonda ICMP della versione 10.1.1.1 destinata alla versione 10.1.4.2.



Nota: In queste richieste, il valore TTL=2 (condizione non rilevabile con debug). Il dispositivo 11A riduce il valore TTL a 1 e inoltra i pacchetti UDP al dispositivo 7A. Il dispositivo 7A azzera il valore TTL e risponde con i messaggi ICMP "time exceeded" (tempo scaduto).

<#root>

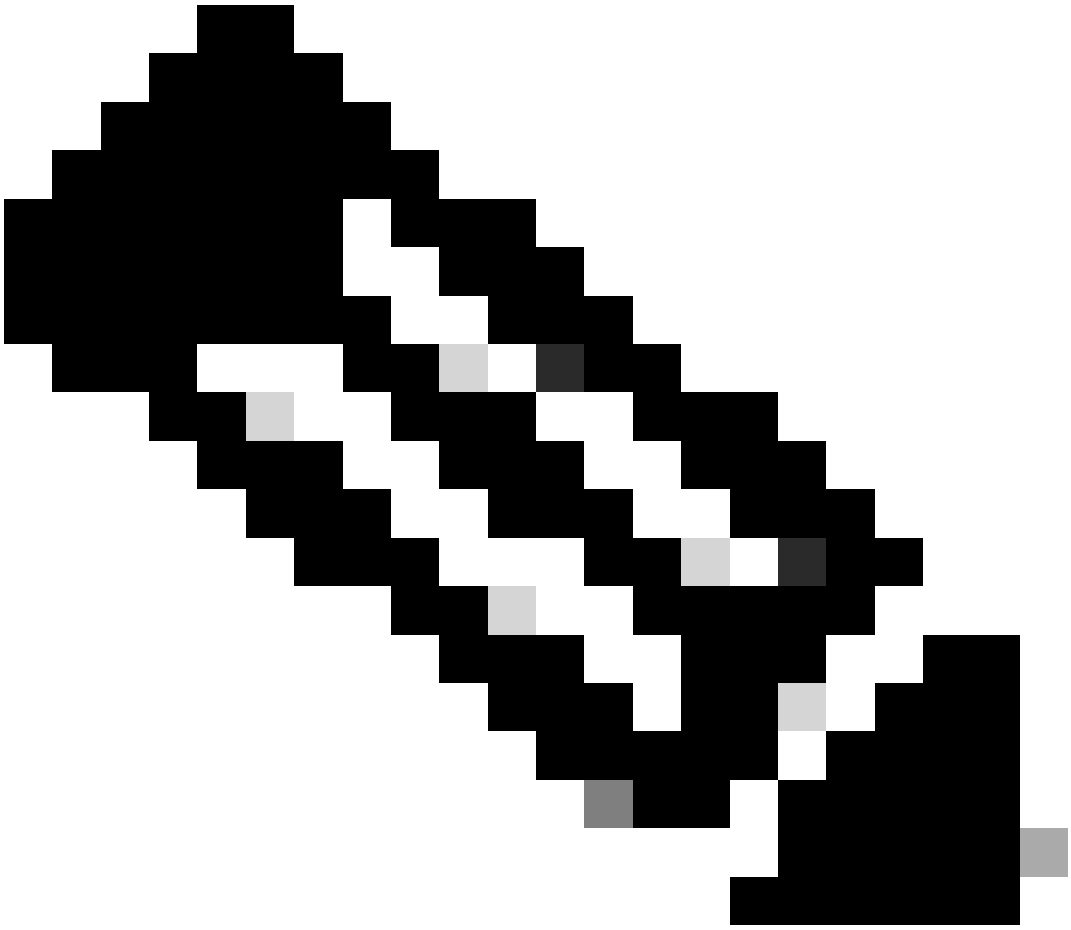
```
*Dec 29 14:02:37.776: IP: s=10.1.1.1 (Ethernet4/0), d=10.1.4.2 (FastEthernet0/0),
 g=10.1.2.2, len 92, forward
*Dec 29 14:02:37.776: ICMP type=8, code=0
*Dec 29 14:02:37.776: IP: s=10.1.3.2 (FastEthernet0/0), d=10.1.1.1 (Ethernet4/0),
 g=10.1.1.1, len 56, forward
*Dec 29 14:02:37.776: ICMP type=11,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

Nell'output del comando debug, vengono visualizzate le tre richieste ICMP successive. Il valore TTL di queste sonde è 3. Il dispositivo 11A riduce il valore TTL a 2 e lo inoltra al dispositivo 7A. Il dispositivo 7A riduce il valore TTL a 1 e inoltra i pacchetti al dispositivo 7B, che riduce il valore TTL a zero e risponde con i messaggi ICMP "tempo scaduto".

<#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
```

Questo output di debug visualizza le ultime tre richieste ICMP. Il valore TTL originale di queste sonde era 4. Il valore TTL è stato diminuito a 3 dal dispositivo 11A, quindi è stato diminuito a 2 dal dispositivo 7A, infine è stato diminuito a 1 dal dispositivo 7B. Il dispositivo 7C risponde quindi con messaggi di risposta echo ICMP (tipo=0, codice=0), poiché era la destinazione delle sonde.



> Nota: I messaggi ICMP di risposta echo non hanno limitazioni di velocità a causa dei messaggi ICMP "porta non raggiungibile". In questo caso, vengono visualizzati tutti e tre i messaggi di risposta echo ICMP inviati.

Note aggiuntive

Sui router Cisco, i codici per una risposta al comando traceroute sono:

```
! -- 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 si esegue il comando traceroute da UNIX, tenere presente quanto segue:

- Puoi ricevere traceroute: icmp socket: Permission denied messaggi.
- Il programma traceroute si basa sul NIT (Network Interface Tap) per snoopare nella rete. Il dispositivo è accessibile solo dalla directory principale. È necessario eseguire il programma come utente root o impostare l'ID utente per il programma root.

Riepilogo

In questo documento viene mostrato come il comando traceroute determina il percorso di un pacchetto da una determinata origine a una determinata destinazione con l'uso di pacchetti UDP e ICMP. I possibili tipi di messaggi ICMP negli output sono:

- Se il valore TTL viene superato durante il transito, digitare=11, codice=0, il pacchetto viene rimandato indietro dal router di transito in tutti i casi in cui il valore TTL dei pacchetti della sonda scade prima che i pacchetti raggiungano la destinazione.
- Se la porta non è raggiungibile, digitare=3, codice=3, il pacchetto viene rinviato in risposta ai pacchetti di richieste UDP quando raggiungono la destinazione (l'applicazione UDP non è definita). Questi pacchetti sono limitati a un pacchetto ogni 500 ms. Questo spiega perché la risposta dalla destinazione (vedere gli output per il router Cisco e Linux) non è riuscita nelle risposte pari. La periferica 7C non genera il messaggio ICMP e l'output del traceroute comando in ciascuna periferica attende più di un secondo. Nel caso dell'output del comando MS Windows tracert , il messaggio ICMP viene generato perché la porta UDP 137 non esiste in un router Cisco.
- Se è presente un'eco, digitare=8, codice=0, il pacchetto di sonda echo viene inviato dal PC con MS Windows.
- Se è presente una risposta echo, tipo=0, codice=0, quando si raggiunge la destinazione viene inviata una risposta al pacchetto precedente. Questa operazione è valida solo per il comando MS Windows tracert .

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione
Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).