Uso del comando traceroute nei vari sistemi operativi

Sommario

Introduzione

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

Prerequisiti

Requisiti

I lettori di questo documento devono avere conoscenze 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 12.2(27)
- PC con Red Hat Linux versione 9
- PC con MS Windows 2000

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.

Funzionamento generale

Se si esegue il comando **traceroute** *ip-address* su un dispositivo di origine (ad esempio un host o un router che agisce da host), il router invia i pacchetti IP alla destinazione con valori TTL (Time To Live) che aumentano 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

Il modo in cui il comando **traceroute** viene implementato nei vari sistemi operativi menzionati in questo documento presenta alcune differenze.

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 comando traceroute esteso). La porta UDP di destinazione della sonda del datagramma iniziale è impostata su 33434 (o come specificato nell'output del comando **traceroute** esteso). Il comando **traceroute** esteso è una variante del normale comando **traceroute** che permette di modificare i valori predefiniti dei parametri usati dall'operazione **traceroute**, ad esempio il numero di porta di destinazione e il valore TTL. Per ulteriori informazioni su come usare il comando **traceroute** esteso, consultare il documento sull'uso del ping esteso e dei comandi estesi di tracciamento routing. 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 comando **traceroute** esteso). Per ciascuna 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 ("destination unreachable", "port unreachable"), che indica che è stato raggiunto un host.un messaggio di tipo "host unreachable", "net unreachable", "maximum TTL exceeded" (TTL massimo superato) o "timeout" (timeout), per segnalare che 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 inviano il messaggio ICMP "tempo scaduto" alla sorgente da cui è stato ricevuto il pacchetto UDP/ICMP.

Il comando Linux **traceroute** è simile all'implementazione del router Cisco. Tuttavia, utilizza una porta di origine fissa. L'opzione *-n* nel comando **traceroute** viene usata per evitare una richiesta a un name server.

Microsoft Windows

Il comando **tracert di** 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 hop_massimi	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:

```
ip icmp rate-limit unreachable  [DF] <1-4294967295 millisecond>

no ip icmp rate-limit unreachable [DF] (DF limits rate for code=4)
```

Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCdp28161 (solo utenti registrati).

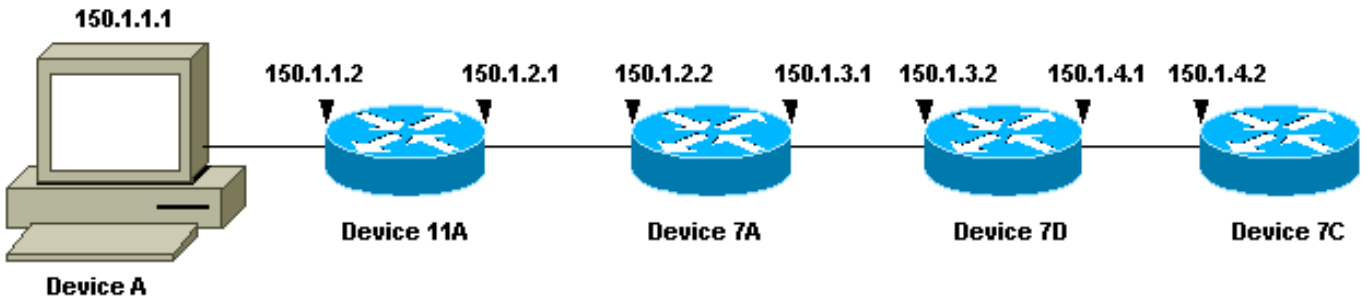
Come mostrato nell'output, questa limitazione si riferisce alla velocità aggregata di tutti gli elementi ICMP non raggiungibili. Per ulteriori informazioni, fare riferimento alla RFC 792 .

```
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 influisce su altri pacchetti come le richieste echo ICMP o i messaggi ICMP "tempo scaduto".

Esempi

Questa topologia di rete viene utilizzata per gli esempi:



In ognuno dei tre esempi viene utilizzato un dispositivo A diverso. Dal dispositivo A, il comando **traceroute 150.1.4.2** 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

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

```
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
```

In questo output di debug, il dispositivo 11A invia messaggi ICMP "tempo scaduto" all'origine delle sonde (150.1.1.1). 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 "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.

```
*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
```

Questo output di debug visualizza la sonda UDP dall'origine 150.1.1.1 destinata a 150.1.4.2.

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 messaggi ICMP "tempo scaduto".

```
*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
```

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 messaggi ICMP "tempo scaduto".

```
*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
```

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 e infine 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 "port unreachable" (porta non raggiungibile) a causa della limitazione della velocità.

PC con 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
```

In questo output di debug, il dispositivo 11A invia messaggi ICMP "tempo scaduto" all'origine delle sonde (150.1.1.1). 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 "tempo scaduto".

Nota: le sonde 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.

```
*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
```

Nota: in questo output di debug, è ora possibile vedere la sonda UDP dall'origine 150.1.1.1 destinata a 150.1.4.2.

Nota: in queste richieste il valore TTL=2 (questo valore non può essere visualizzato 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 messaggi ICMP "tempo scaduto".

```
*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
```

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 messaggi ICMP "tempo scaduto".

```
*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
```

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 e infine a 1 dal dispositivo 7B. Il dispositivo 7C risponde quindi con messaggi ICMP "port unreachable" (porta non raggiungibile), dal momento che era la destinazione delle sonde.

Nota: il dispositivo 7C invia solo due messaggi ICMP "port unreachable" (porta non raggiungibile) a causa della limitazione della velocità.

PC con 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
```

In questo output di debug, il dispositivo 11A invia messaggi ICMP "tempo scaduto" all'origine delle sonde (150.1.1.1). 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 visualizzati i nomi NETBIOS richiesti. 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 usare l'opzione *-d* nel comando **tracert** per disabilitare il comportamento NETBIOS.

Nota: le sonde ICMP non vengono visualizzate in questo output di **debug** per due motivi:

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

```
*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
```

In questo output di debug, è ora possibile vedere la sonda ICMP della sorgente 150.1.1.1 destinata a 150.1.4.2.

Nota: in queste richieste, il valore TTL=2 (questo non può essere visualizzato 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 messaggi ICMP "tempo scaduto".

```
*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
```

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 messaggi ICMP "tempo scaduto".

```
*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
```

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 e infine 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 una frequenza limitata, a differenza dei messaggi ICMP "port unreachable" (porta non raggiungibile). In questo caso, vengono visualizzati tutti e tre i messaggi di risposta echo ICMP inviati.

Note aggiuntive

Nei 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:

- si potrebbe ricevere il messaggio di errore "traceroute: socket icmp: Permission negato".
- 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 inviato 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 comando **traceroute** in ciascuna periferica attende più di un secondo. Nel caso dell'output del comando **tracert di** MS Windows, 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 MS Windows.
- Se è presente una risposta echo, tipo=0, codice=0, quando si raggiunge la destinazione viene inviata una risposta al pacchetto precedente. Questo vale solo per il comando **tracert di** MS Windows.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems