

Verwenden des Befehls traceroute auf Betriebssystemen

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Allgemeiner Betrieb](#)

[Cisco IOS und Linux](#)

[Microsoft Windows](#)

[Durchsatzbegrenzung für ICMP Unreachables](#)

[Beispiele](#)

[Cisco Router mit Cisco IOS-Software](#)

[PC mit Linux](#)

[PC mit MS Windows](#)

[Zusätzliche Hinweise](#)

[Zusammenfassung](#)

[Zugehörige Informationen](#)

Einführung

Mit dem Befehl **traceroute** können Sie den Pfad eines Pakets bestimmen, um von einer bestimmten Quelle zu einem Ziel zu gelangen, indem Sie die Sequenz von Hops zurückgeben, die das Paket durchlaufen hat. Dieses Dienstprogramm ist im Lieferumfang Ihres Host-Betriebssystems (z. B. Linux oder Microsoft (MS) Windows) sowie der Cisco IOS® Software enthalten.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten über grundlegende Kenntnisse eines der folgenden Betriebssysteme verfügen:

- Cisco IOS-Software
- Linux
- Microsoft Windows

Verwendete Komponenten

Die Informationen in diesem Dokument gelten für die folgenden Software- und Hardwareversionen:

- Cisco Router mit Cisco IOS Software-Version 12.2(27)
- PC, auf dem Red Hat Linux Version 9 ausgeführt wird
- PC mit MS Windows 2000

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

Allgemeiner Betrieb

Wenn Sie den **Befehl `traceroute ip-address`** auf einem Quellgerät (z. B. einem Host oder einem Router, der als Host fungiert) ausführen, sendet er IP-Pakete mit TTL-Werten (Time To Live) an das Ziel, die bis zur maximal angegebenen Hop-Anzahl erhöht werden. Dies ist standardmäßig 30. In der Regel senkt jeder Router im Pfad zum Ziel das TTL-Feld um eine Einheit, während er diese Pakete weiterleitet. Wenn ein Router in der Mitte des Pfads ein Paket mit TTL = 1 findet, reagiert er mit einer ICMP-Meldung (Internet Control Message Protocol), die die Zeit überschritten hat, an die Quelle. Diese Meldung informiert die Quelle, dass das Paket diesen bestimmten Router als Hop durchläuft

Es gibt einige Unterschiede hinsichtlich der Implementierung des Befehls **traceroute** in den verschiedenen Betriebssystemen, die in diesem Dokument behandelt werden.

Cisco IOS und Linux

Die TTL für die UDP-Datagramm-Datensammlungsprüfung (User Datagram Protocol) ist auf 1 (oder die minimale TTL, wie vom Benutzer im erweiterten **Befehl `traceroute`** festgelegt. Der Ziel-UDP-Port der anfänglichen Datagramm-Anfrage ist auf 33434 (oder wie in der erweiterten **Traceroute-Befehlsausgabe** angegeben) festgelegt. Der Befehl **traceroute** erweitert ist eine Variante des Befehls **traceroute**, mit dem die Standardwerte der Parameter, die von der **Traceroute-Operation** wie TTL und Zielportnummer verwendet werden, geändert werden können. Weitere Informationen zur Verwendung des erweiterten **traceroute**-Befehls finden Sie unter [Verwenden der Befehle `Extended ping` und `Extended Traceroute`](#). Der Quell-UDP-Port der anfänglichen Datagramm-Anfrage ist randomisiert und verfügt über einen logischen Operator OR mit 0x8000 (stellt einen minimalen Quellport von 0x8000 sicher). Diese Schritte veranschaulichen, was beim Start des UDP-Datagramms geschieht:

Hinweis: Die Parameter können konfiguriert werden. Dieses Beispiel beginnt mit $n = 1$ und endet mit $n = 3$.

1. Das UDP-Datagramm wird mit TTL = 1, Ziel-UDP-Port= 33434 und dem Quell-Port

randomisiert.

2. Der UDP-Zielport wird erhöht, der Quell-UDP-Port randomisiert und das zweite Datagramm gesendet.
3. Schritt 2 wird für bis zu drei Probes wiederholt (oder so oft, wie in einer erweiterten **Traceroute**-Befehlsausgabe gefordert). Für jede gesendete Probe erhalten Sie eine "TTL exceeded"-Nachricht, die verwendet wird, um einen schrittweisen Pfad zum Ziel-Host zu erstellen.
4. TTL wird erhöht, und dieser Zyklus wiederholt sich mit inkrementellen Ziel-Portnummern, wenn die ICMP-Meldung "time exceeded" (Zeit überschritten) empfangen wird. Sie können auch eine der folgenden Meldungen erhalten: Eine ICMP-Meldung vom Typ 3, Code 3 ("destination unreachable", "port unreachable"), die angibt, dass ein Host erreicht wurde. Ein "Host unreachable", "net unreachable", "maximum TTL exceeded" (maximale TTL überschritten) oder ein "timeout"-Meldungstyp, d. h. die Anfrage wird erneut gesendet.

Cisco Router senden UDP-Testpakete mit einem zufälligen Quell-Port und einem inkrementellen Zielport (zur Unterscheidung der verschiedenen Sonden). Cisco Router senden die ICMP-Meldung "time exceeded" (Zeit überschritten) zurück an die Quelle, von der das UDP-/ICMP-Paket empfangen wurde.

Der Linux-**Traceroute**-Befehl ähnelt der Cisco Router-Implementierung. Es wird jedoch ein fester Quellport verwendet. Die *-n*-Option im Befehl **traceroute** wird verwendet, um eine Anforderung an einen Namensserver zu vermeiden.

Microsoft Windows

Der MS Windows **tracert**-Befehl verwendet ICMP-Echo-Anforderungsdatagramme anstelle von UDP-Datagrammen als Tests. ICMP-Echoanfragen werden mit inkrementierendem TTL gestartet, und der gleiche Vorgang, der in [Cisco IOS und Linux](#) beschrieben wird, wird ausgeführt. Die Verwendung von ICMP-Echo-Anforderungsdatagrammen hat den Zweck, dass der letzte Hop nicht auf die Antwort einer "nicht erreichbaren" ICMP-Nachricht vom Zielhost angewiesen ist. Stattdessen ist eine ICMP-Echo-Antwortnachricht erforderlich.

Die Befehlsyntax lautet:

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

In dieser Tabelle werden die Befehlsparameter erläutert:

Parameter	Beschreibung
-d	Gibt an, dass Adressen nicht auf Computernamen aufgelöst werden sollen.
-h maximum_hops	Gibt die maximale Anzahl von Hops an, die nach einem Ziel gesucht werden sollen.
-j Computerliste	Gibt eine lose Quellroute entlang der Computerliste an.
-w Timeout	Wartet auf die durch das Timeout angegebene Anzahl von Millisekunden für jede Antwort.
Zielname	Name des Zielcomputers.

Durchsatzbegrenzung für ICMP Unreachables

ICMP Unreachables sind auf ein Paket pro 500 ms (als Schutz vor DoS-Angriffen) in einem Cisco Router beschränkt. Ab Cisco IOS Software Release 12.1 und höher ist dieser Ratenwert konfigurierbar. Der eingeführte Befehl lautet:

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

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

Weitere Informationen finden Sie unter Cisco Bug ID [CSCdp28161](#) (nur [registrierte](#) Kunden).

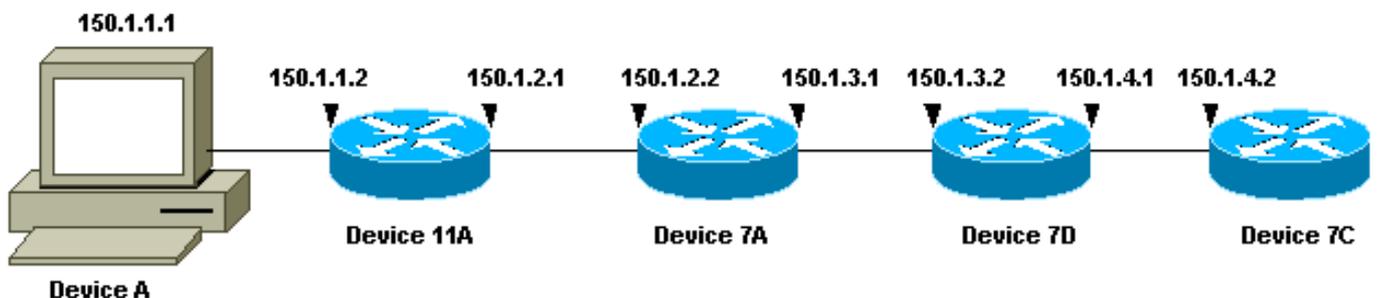
Diese Einschränkung gilt für die Gesamtrate aller nicht erreichbaren ICMP-Dateien, wie diese Ausgabe zeigt. Weitere Informationen finden Sie in [RFC 792](#).

```
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.
```

Diese Einschränkung betrifft keine anderen Pakete wie ICMP-Echoanfragen oder ICMP-Meldungen, die die Zeit überschritten haben.

Beispiele

Diese Netzwerktopologie wird für die folgenden Beispiele verwendet:



In jedem der drei Beispiele wird ein anderes Gerät A verwendet. Von Gerät A wird der Befehl **traceroute 150.1.4.2** auf Gerät 7C ausgeführt.

In jedem der Beispiele wird der Befehl **debug ip packet detail** auf Gerät 11A ausgeführt.

Cisco Router mit Cisco IOS-Software

Dieses erweiterte **Traceroute**-Befehlsbeispiel zeigt die Optionen, die Sie ändern können, wenn Sie einen **Traceroute**-Befehl von einem Cisco Router ausführen. In diesem Beispiel wird alles standardmäßig übernommen:

```
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 dieser Debug-Ausgabe sendet Gerät 11A ICMP-Meldungen, die die Zeit überschritten haben, an die Quelle der Sonden (150.1.1.1). Diese ICMP-Meldungen werden als Antwort auf die ersten Tests mit TTL=1 angezeigt. Gerät 11A senkt die TTL auf Null und antwortet mit den "zeitüberschreitenden" Nachrichten.

Hinweis: Die UDP-Tests werden in dieser Debugausgabe aus zwei Gründen nicht angezeigt:

- Gerät 11A ist nicht das Ziel der UDP-Tests.
- Die TTL wird auf Null herabgesetzt, und das Paket wird nie geroutet. Daher erkennt das Debuggen das Paket nie.

```
*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
```

Diese Debug-Ausgabe zeigt die UDP-Abfrage aus der Quelle 150.1.1.1, die für 150.1.4.2

bestimmt ist.

Hinweis: Bei diesen Tests ist TTL=2 (dies ist beim Debuggen nicht sichtbar). Gerät 11A senkt die TTL auf 1 und leitet die UDP-Pakete an Gerät 7A weiter. Gerät 7A senkt die TTL auf Null und antwortet mit ICMP-Nachrichten, die die Zeit überschritten haben.

```
*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
```

Die nächsten drei UDP-Tests werden in dieser Debugausgabe angezeigt. Die TTL für diese Proben ist 3. Gerät 11A senkt die TTL auf 2 und leitet sie an Gerät 7A weiter. Gerät 7A senkt die TTL auf 1 und leitet die Pakete an Gerät 7B weiter, das die TTL auf Null herabsetzt und mit ICMP-Meldungen "Time exceeded" (Zeitüberschreitung) antwortet.

```
*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
```

Sie können die letzten drei UDP-Tests in dieser Debugausgabe sehen. Die ursprüngliche TTL dieser Proben betrug 4. Die TTL wurde von Gerät 11A auf 3 herabgesetzt, dann von Gerät 7A auf 2 herabgesetzt und dann von Gerät 7B auf 1 herabgesetzt. Gerät 7C antwortet mit ICMP-Meldungen "port unreachable" (Port nicht erreichbar), da es das Ziel der Proben war.

Hinweis: Gerät 7C sendet aufgrund der Ratenbeschränkung nur zwei ICMP-Meldungen "Port unreachable" (Port nicht erreichbar).

```
[root#linux-pc]#tracert -n 150.1.4.2
tracert 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 dieser Debug-Ausgabe sendet Gerät 11A ICMP-Meldungen, die die Zeit überschritten haben, an die Quelle der Sonden (150.1.1.1). Diese ICMP-Meldungen werden als Antwort auf die ersten Tests mit TTL=1 angezeigt. Gerät 11A senkt die TTL auf Null und antwortet mit den "zeitüberschreitenden" Nachrichten.

Hinweis: Die UDP-Tests werden in dieser Debugausgabe aus zwei Gründen nicht angezeigt:

- Gerät 11A ist nicht das Ziel der UDP-Tests.
- Die TTL wird auf Null herabgesetzt, und das Paket wird nie geroutet. Daher erkennt das Debuggen das Paket nie.

```
*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
```

Hinweis: In dieser Debugausgabe sehen Sie jetzt die UDP-Abfrage aus Quelle 150.1.1.1, die für 150.1.4.2 bestimmt ist.

Hinweis: Bei diesen Tests ist TTL=2 (dies ist beim Debuggen nicht sichtbar). Gerät 11A senkt die TTL auf 1 und leitet die UDP-Pakete an Gerät 7A weiter. Gerät 7A senkt die TTL auf Null und antwortet mit ICMP-Nachrichten, die die Zeit überschritten haben.

```
*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

```

Die nächsten drei UDP-Tests werden jetzt in dieser Debugausgabe angezeigt. Die TTL für diese Proben ist 3. Gerät 11A senkt die TTL auf 2 und leitet sie an Gerät 7A weiter. Gerät 7A senkt die TTL auf 1 und leitet die Pakete an Gerät 7B weiter, das die TTL auf Null herabsetzt und mit ICMP-Meldungen "Time exceeded" (Zeitüberschreitung) antwortet.

```

*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

```

Diese Debugausgabe zeigt die letzten drei UDP-Tests. Die ursprüngliche TTL dieser Proben betrug 4. Die TTL wurde von Gerät 11A auf 3 herabgesetzt, dann von Gerät 7A auf 2 herabgesetzt und dann von Gerät 7B auf 1 herabgesetzt. Gerät 7C antwortet dann mit "Port unreachable"-ICMP-Meldungen, da es das Ziel der Proben war.

Hinweis: Gerät 7C sendet aufgrund der Ratenbegrenzung nur zwei ICMP-Meldungen "Port unreachable" (Port nicht erreichbar).

[PC mit 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 dieser Debug-Ausgabe sendet Gerät 11A ICMP-Meldungen, die die Zeit überschritten haben, an die Quelle der Sonden (150.1.1.1). Diese ICMP-Meldungen reagieren auf die anfänglichen Tests, bei denen es sich um ICMP-Echoanforderungspakete mit einem TTL=1 handelt. Gerät 11A senkt die TTL auf Null und antwortet mit den ICMP-Nachrichten.

Hinweis: Oben sehen Sie die Namensanforderungen für das NETBIOS. Diese Anforderungen werden als UDP-Pakete mit Quell- und Zielports von 137 angesehen. Aus Gründen der Klarheit werden die NETBIOS-Pakete vom Rest der Debug-Ausgabe entfernt. Sie können die Option `-d` im Befehl `tracert` verwenden, um das NETBIOS-Verhalten zu deaktivieren.

Hinweis: Die ICMP-Tests werden in dieser **Debugausgabe** aus zwei Gründen nicht angezeigt:

- Gerät 11A ist nicht das Ziel der ICMP-Tests.
- Die TTL wird auf Null herabgesetzt, und das Paket wird nie geroutet. Daher erkennt das Debuggen das Paket nie.

```

*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 dieser Debug-Ausgabe sehen Sie nun den ICMP-Test aus Quelle 150.1.1.1, der auf 150.1.4.2 ausgerichtet ist.

Hinweis: Bei diesen Tests ist TTL=2 (dies ist beim Debuggen nicht sichtbar). Gerät 11A senkt die TTL auf 1 und leitet die UDP-Pakete an Gerät 7A weiter. Gerät 7A senkt die TTL auf Null und antwortet mit ICMP-Nachrichten, die die Zeit überschritten haben.

```
*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
```

Die nächsten drei ICMP-Tests werden in dieser Debugausgabe angezeigt. Die TTL für diese Proben ist 3. Gerät 11A senkt die TTL auf 2 und leitet sie an Gerät 7A weiter. Gerät 7A senkt die TTL auf 1 und leitet die Pakete an Gerät 7B weiter, das die TTL auf Null herabsetzt und mit ICMP-Meldungen "Time exceeded" (Zeitüberschreitung) antwortet.

```
*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
```

Diese Debugausgabe zeigt die letzten drei ICMP-Tests. Die ursprüngliche TTL dieser Proben betrug 4. Die TTL wurde von Gerät 11A auf 3 herabgesetzt, dann von Gerät 7A auf 2 herabgesetzt und dann von Gerät 7B auf 1 herabgesetzt. Gerät 7C antwortet dann mit ICMP-Echo-Antwortnachrichten (type=0, code=0), da es das Ziel der Proben war.

Hinweis: Die ICMP-Echo-Antwortnachrichten sind nicht begrenzt, da die ICMP-Meldungen "port

unreachable" (Port nicht erreichbar) verwendet wurden. In diesem Fall werden alle drei ICMP-Echo-Antwortnachrichten gesendet.

Zusätzliche Hinweise

Bei Cisco Routern lauten die Codes für eine **Traceroute**-Befehlsantwort:

```
! -- 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)
```

Wenn Sie den Befehl **traceroute** von UNIX ausführen, notieren Sie sich die folgenden Elemente:

- Sie können "traceroute: ICMP-Sockel: Nachrichten mit verweigerter Genehmigung".
- Das **Traceroute**-Programm verwendet die Network Interface Tap (NIT), um im Netzwerk zu schnüffeln. Auf dieses Gerät kann nur über root zugegriffen werden. Sie müssen das Programm entweder als root ausführen oder die Benutzer-ID als root festlegen.

Zusammenfassung

Dieses Dokument hat gezeigt, wie der Befehl **traceroute** den Pfad festlegt, den ein Paket mithilfe von UDP- und ICMP-Paketen von einer bestimmten Quelle zu einem bestimmten Ziel führt. Die möglichen Arten von ICMP-Meldungen in den Ausgaben sind:

- Wenn die TTL bei der Übertragung überschritten wird, type=11, code=0, dann wird das Paket vom Transit-Router in allen Fällen zurückgesendet, in denen die TTL der Testpakete abläuft, bevor die Pakete das Ziel erreichen.
- Wenn der Port nicht erreichbar ist, geben Sie type=3, code=3 ein, dann wird das Paket als Antwort auf die UDP-Prüfpakete zurückgesendet, wenn sie das Ziel erreichen (die UDP-Anwendung ist nicht definiert). Diese Pakete sind auf ein Paket pro 500 ms beschränkt. Dies erklärt, warum die Antwort vom Ziel (siehe die Ausgaben für den [Cisco Router](#) und [Linux](#)) in den geraden Antworten fehlschlug. Gerät 7C generiert die ICMP-Meldung nicht, und die Ausgabe des **Traceroute**-Befehls in jedem Gerät wartet mehr als eine Sekunde. Bei der Ausgabe des Befehls **tracert** MS Windows wird die ICMP-Meldung generiert, da der UDP-Port 137 in einem Cisco Router nicht vorhanden ist.
- Wenn ein Echo vorhanden ist, type=8, code=0, wird das Echo-Probe-Paket vom MS Windows-PC gesendet.
- Wenn eine Echo-Antwort vorliegt, geben Sie=0, code=0 ein, dann wird eine Antwort auf das vorherige Paket gesendet, wenn das Ziel erreicht ist. Dies gilt nur für den MS Windows **tracert**-Befehl.

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)