



شبکه‌های مخابراتی

سید حمید صفوی

دانشکده فنی و مهندسی

دانشگاه محقق اردبیلی

نیمسال دوم ۹۸-۹۹

جستجوی درون شبکه به وسیله Traceroute

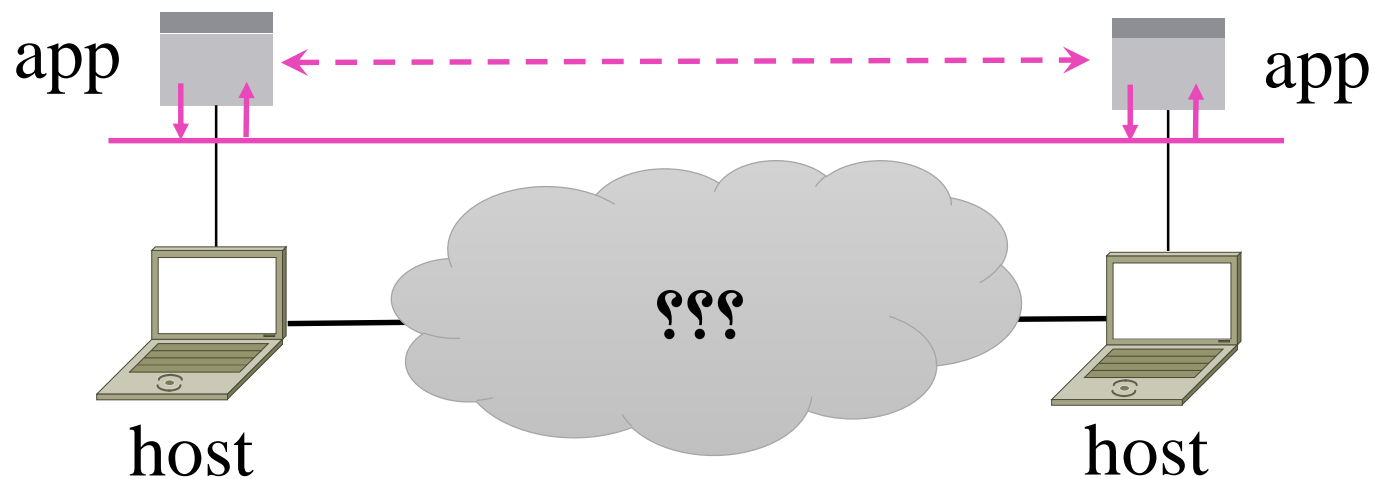
Traceroute Command

```
mtr -n --report 8.8.8.8
HOST: example
  1. |--- 192.168.0.1          0.0%  10    9.4   7.5   3.1  11.7  2.8
  2. |--- 10.89.0.1          0.0%  10   13.1  24.4  11.7  69.9  21.7
  3. |--- 173.212.126.117    0.0%  10   22.0  20.7  13.0  26.5   4.5
  4. |--- 24.215.102.161     0.0%  10   29.2  28.1  23.4  31.9   2.9
  5. |--- 24.215.102.221     0.0%  10   22.0  26.1  22.0  30.1   3.1
  6. |--- 24.215.102.9       0.0%  10   25.8  27.2  22.2  33.7   3.5
  7. |--- 24.215.101.10      0.0%  10  107.8  52.1  41.5 107.8  19.8
  8. |--- 209.85.250.3       0.0%  10   68.0  48.6  42.1  68.0   7.3
  9. |--- 8.8.8.8            0.0%  10   42.9  47.3  42.8  56.0   4.2
```



سرویس شبکه API جزئیات را پنهان می کند

- برنامه‌ها بدون اطلاع از آنچه که درون شبکه وجود دارد با هم در ارتباط هستند.
- این خوب است! اما شما ممکن است کنجکاو باشید ...



Traceroute

Van Jacobson

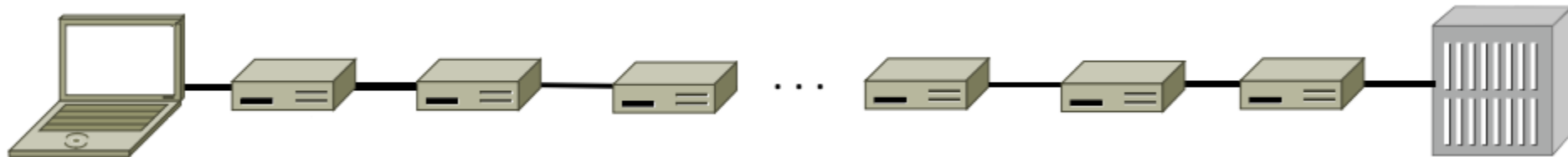


Credit: Wikipedia (public domain)

- به طور گسترده‌ای از ابزار خط فرمان (Command Line) استفاده می‌شود که به میزبانان (hosts) اجازه می‌دهد تا درون شبکه جستجو کنند.
- روی تمام سیستم عامل‌ها (tracert on windows)
- طراحی شده توسط Van Jacobson ~ 1987
- استفاده از رابط شبکه - شبکه (IP) به نحوی که بعداً توضیح داده خواهد شد.

Traceroute (2)

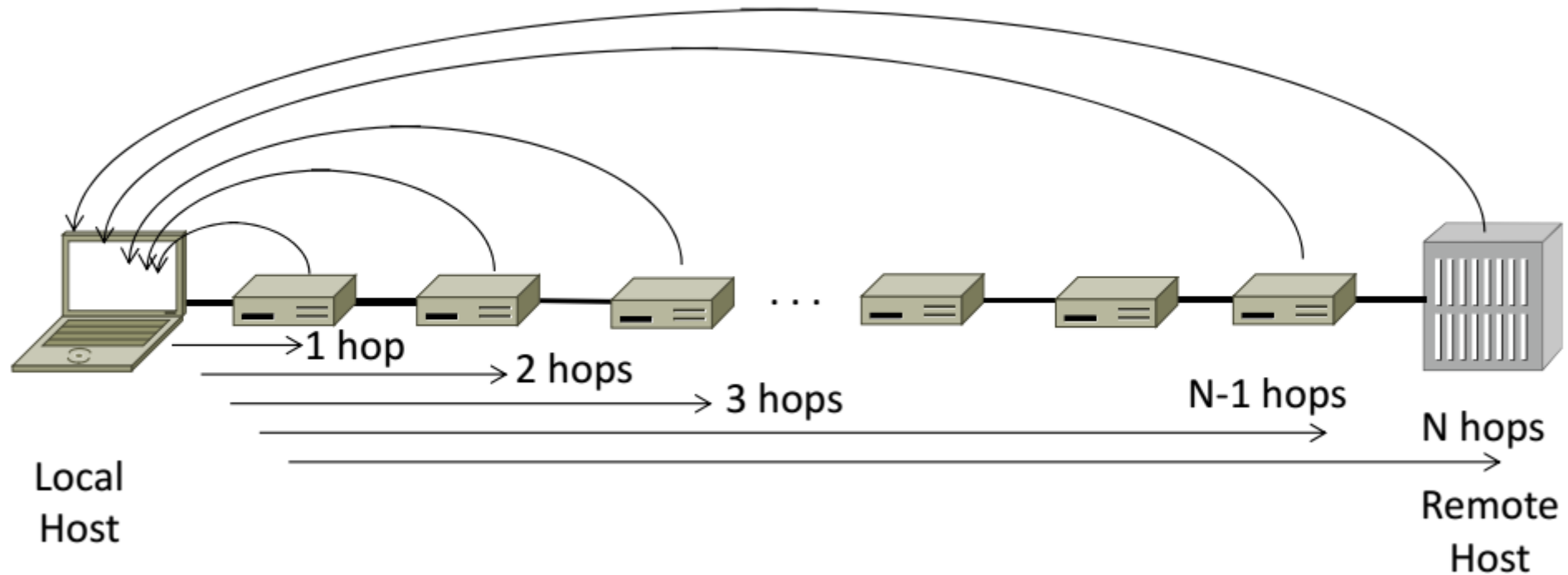
- جست و جوی متوالی پرش‌ها برای پیدا کردن یک مسیر خاص در شبکه.



میزبان محلی

میزبان راه دور

Traceroute (3)



استفاده از Traceroute

- Tracert < host name >
- Tracert < IP Address >

- Tracert www.uw.edu

مثال:



استفاده از Traceroute

```
Administrator: Command Prompt
C:\Users\djw>tracert www.uw.edu

Tracing route to www.washington.edu [128.95.155.134]
over a maximum of 30 hops:

  0  1 ms    <1 ms   2 ms   192.168.1.1
  1  8 ms    8 ms    9 ms   88.Red-80-58-67.staticIP.rima-tde.net [80.58.67.88]
  2 16 ms    5 ms   11 ms  169.Red-80-58-78.staticIP.rima-tde.net [80.58.78.169]
  3 12 ms   12 ms  13 ms  217.Red-80-58-87.staticIP.rima-tde.net [80.58.87.217]
  4  5 ms    11 ms   6 ms   et-1-0-0-1-101-GRIBCNE1.red.telefonica-wholesale.net [94.142.103.205]
  5 40 ms   38 ms  38 ms  176.52.250.226
  6 108 ms  106 ms 136 ms xe-6-0-2-0-grtnycpt2.red.telefonica-wholesale.net [213.140.43.9]
  7 180 ms  179 ms 182 ms Xe9-2-0-0-grtpaopx2.red.telefonica-wholesale.net [94.142.118.178]
  8 178 ms  175 ms 176 ms te-4-2-car1.SanJose2.Level3.net [4.59.0.225]
  9 190 ms  186 ms 187 ms vlan80.csw3.SanJose1.Level3.net [4.69.152.190]
 10 185 ms  185 ms 187 ms ae-82-82.ebr2.SanJose1.Level3.net [4.69.153.25]
 11 268 ms  205 ms 207 ms ae-7-7.ebr1.Seattle1.Level3.net [4.69.132.50]
 12 334 ms  202 ms 195 ms ae-12-51.car2.Seattle1.Level3.net [4.69.147.132]
 13 195 ms  196 ms 195 ms PACIFIC-NOR.car2.Seattle1.Level3.net [4.53.146.142]
 14 197 ms  195 ms 196 ms ae0--4000.iccr-sttlwa01-02.infra.pnw-gigapop.net [209.124.188.132]
 15 196 ms  196 ms 195 ms v14000.uwbr-ads-01.infra.washington.edu [209.124.188.133]
 16 *      *      *      Request timed out.
 17 201 ms  194 ms 196 ms ae4--583.uwar-ads-1.infra.washington.edu [128.95.155.131]
 18 197 ms  196 ms 195 ms www1.cac.washington.edu [128.95.155.134]

Trace complete.
```



استفاده از Traceroute (۱)

- در خروجی دستور Tracert پنج ستون مشاهده می کنید.
- ستون اول (سمت چپ) شماره هاپها را نشان می دهد.
- ستون آخر IP یا نام هر هاپ را نمایش می دهد.
- اما سه ستون بعد از ستون اول در دستور Tracert چه چیزی را نشان می دهد؟

Tracert برای هر هاپ ۳ بسته ارسال می کند که هر ستون مربوط به هر بسته است. با ارسال این سه بسته، خروجی معتبرتر و قابل اعتمادتری خواهیم داشت. مجموع زمان ارسال هر بسته از کامپیوتر ما به هاپ و دریافت پاسخ از هاپ به کامپیوتر ما (مجموع زمان رفت و برگشت) مقادیری هستند که در این ستونها قرار می گیرند.



استفاده از Traceroute (۲)

- چنانچه برای یک هاپ، بسته ارسالی دچار مشکل شود و به مبدا برنگردد، یک ستاره * بجای زمان، نمایش داده می شود.
- اولین هاپی که در خروجی Tracert قبل مشاهده می کنید، مودم ما با آی پی 192.168.1.1 می باشد. در صورتی که در یک LAN هستید و از طریق یک مودم به اینترنت متصل می شوید اولین هاپ شما **مودم** شما خواهد بود.
- در صورتی که Tracert به مقصد برسد، آخرین هاپ، آدرسی است که آن را Tracert کردید.
- نکته جالب دیگری که در تصویر اسلاید قبل در بررسی خروجی Tracert می توان به آن اشاره کرد، IP های خصوصی هاپها است. این IP ها مربوط به روترهای شبکه اینترنت ISP و مخابرات می باشد.



استفاده از Traceroute (۳)

- با بررسی IP ها می‌توانیم شهرها و کشورهایی را که بسته‌های ما برای رسیدن به مقصد طی می‌کنند بیابیم.

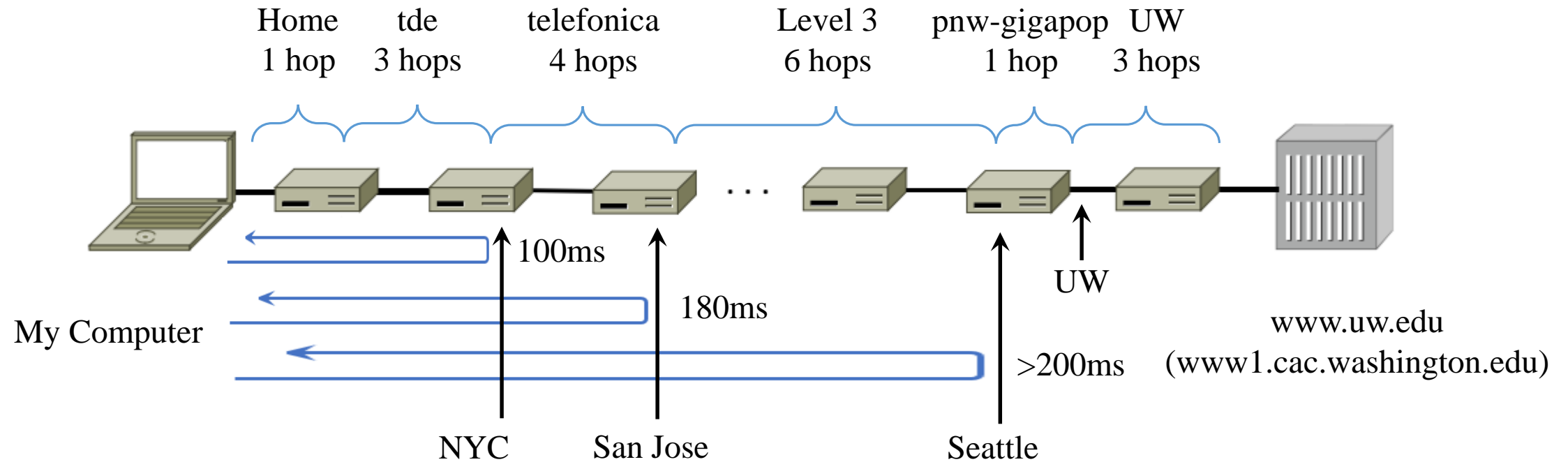
نکته: معمولاً با افزایش تعداد هاپ‌ها زمان Trace شدن نیز افزایش می‌یابد.

- در خط پایان تعداد هاپ‌هایی که از آن‌ها عبور می‌کند مشخص می‌شود.



استفاده از Traceroute (۴)

- نام و مکان ISP ها به طور تجربی برآورد شده‌اند.



خطایابی با استفاده از Traceroute

- اگر در ارتباط بین بخش‌های مختلف اشکالی پیش بیاید چگونه با استفاده از دستور Traceroute آن را کشف کنیم؟

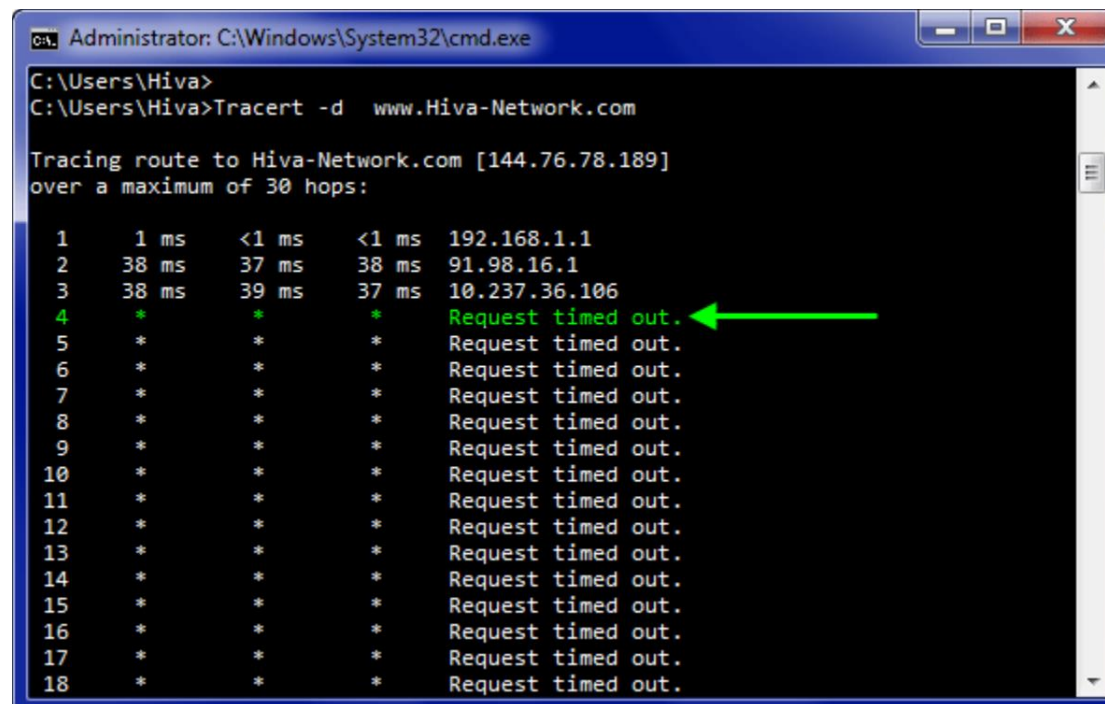
حالت اول: فرض کنید شما دفتر نمایندگی شرکتی در اردبیل هستید. یک روز کاربران از سرعت پایین شبکه شاکی می‌شوند. شما می‌دانید که بسته‌های داده از شرکت شما مستقر در اردبیل تا دفتر مرکزی شرکت در تهران معمولاً ۱۳ هاپ را طی می‌کند.

با استفاده از این دستور متوجه می‌شوید که تعداد هاپ‌ها به ۲۰ عدد افزایش یافته است. این بدان معناست که بسته‌ها مسیر دیگری را برای رسیدن به مقصد طی می‌کنند. به عبارت دیگر مسیری که معمولاً طی می‌شد، ممکن است down شده باشد. دستور Traceroute مسیر جدید را به شما نشان می‌دهد. همچنین قابلیت چک کردن مسیر مشخص را نیز دارد.



خطایابی با استفاده از Traceroute

حالت دوم: ممکن است یکی از روترها دچار مشکل شده باشد. با استفاده از Tracert می‌توان متوجه شد که حداکثر تا کدام روتر (یا روترها) بسته‌های ارسالی بدون مشکل مسیر را طی می‌کنند. اولین روتری که بعد از آن بسته، دیگر پاسخی نداریم جایی است که مشکل از آنجا آغاز می‌شود.



```
Administrator: C:\Windows\System32\cmd.exe
C:\Users\Hiva>
C:\Users\Hiva>Tracert -d www.Hiva-Network.com

Tracing route to Hiva-Network.com [144.76.78.189]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.1.1
  1  38 ms  37 ms  38 ms  91.98.16.1
  2  38 ms  39 ms  37 ms  10.237.36.106
  3  *      *      *      Request timed out.
  4  *      *      *      Request timed out.
  5  *      *      *      Request timed out.
  6  *      *      *      Request timed out.
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
  9  *      *      *      Request timed out.
 10  *      *      *      Request timed out.
 11  *      *      *      Request timed out.
 12  *      *      *      Request timed out.
 13  *      *      *      Request timed out.
 14  *      *      *      Request timed out.
 15  *      *      *      Request timed out.
 16  *      *      *      Request timed out.
 17  *      *      *      Request timed out.
 18  *      *      *      Request timed out.
```



سوئیچ‌های فرمان Traceroute

• Tracert -d

این سوئیچ در هنگام بررسی هاپ‌ها، فقط IP آن‌ها را نشان می‌دهد و نام آن‌ها را Resolve نمی‌کند. این امر باعث افزایش چشم‌گیر سرعت به پایان رسیدن Trace می‌شود. کفایت یک بار بدون -d و یک بار با -d عمل Trace را انجام دهید و سرعت آن‌ها را مقایسه کنید.

• Tracert -h

برای Trace کردن وب سایت دانشگاه واشنگتن، ملاحظه کردید که از ۱۹ هاپ عبور کرد. چنانچه بخواهید فقط تا تعداد معینی از هاپ Trace انجام شود (نه بیشتر) از این سوئیچ استفاده کنید. مثلا می‌توانید مشخص کنید که فقط تا پنج هاپ Trace انجام شود.

Tracert -h 5 www.uw.edu

نکته: به طور پیش فرض تا ۳۰ هاپ نمایش داده خواهد شد.



سوئیچ‌های فرمان Traceroute

• Tracert –w

به کمک این سوئیچ می‌توان حداکثر مدت زمانی را که باید منتظر پاسخ از هاپ بود را تعیین کرد. این مقدار بر حسب میلی‌ثانیه در نظر گرفته می‌شود. به مثال زیر توجه کنید:

Tracert –w 100 www.uw.edu

در این مثال، حداکثر مدت زمان انتظار ۱۰۰ میلی‌ثانیه در نظر گرفته شده است.



مراجع این بخش

• سایت هیوا شبکه به آدرس: <https://www.hiva-network.com>

