شبکه‌های مخابراتی

سید حمید صفوی
دانشکده فنی و مهندسی
دانشگاه محقق اردبیلی
نیمسال دوم ۹۸-۹۹

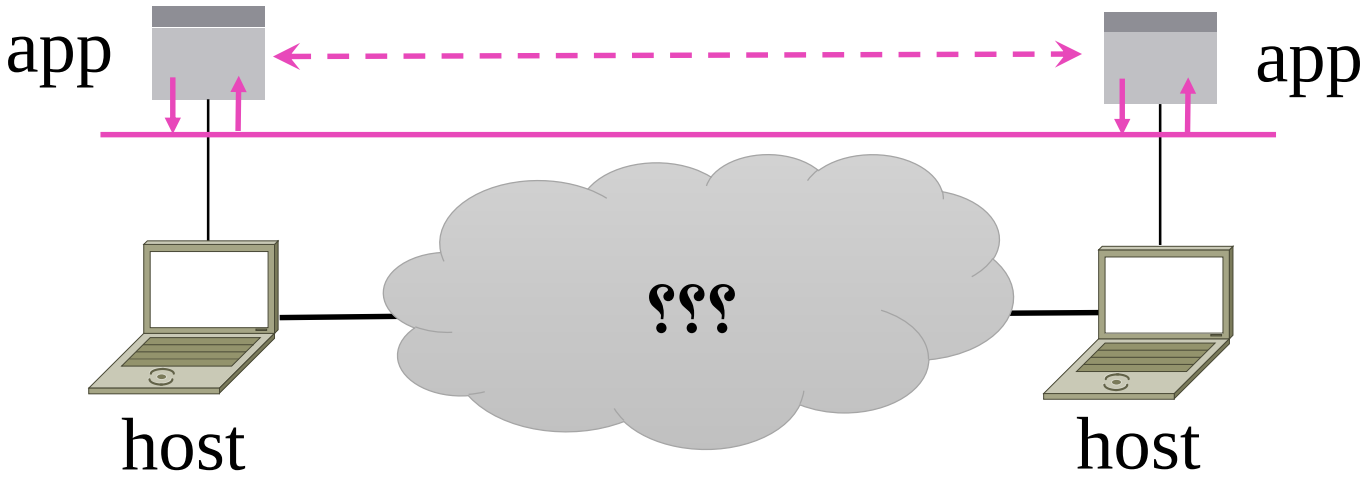
جستجوی درون شبکه به وسیله Traceroute

Traceroute Command

```
mtr -n --report 8.8.8.8
HOST: example                    Loss%   Snt   Last   Avg  Best  Wrst StDev
  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 می‌کند

- 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)

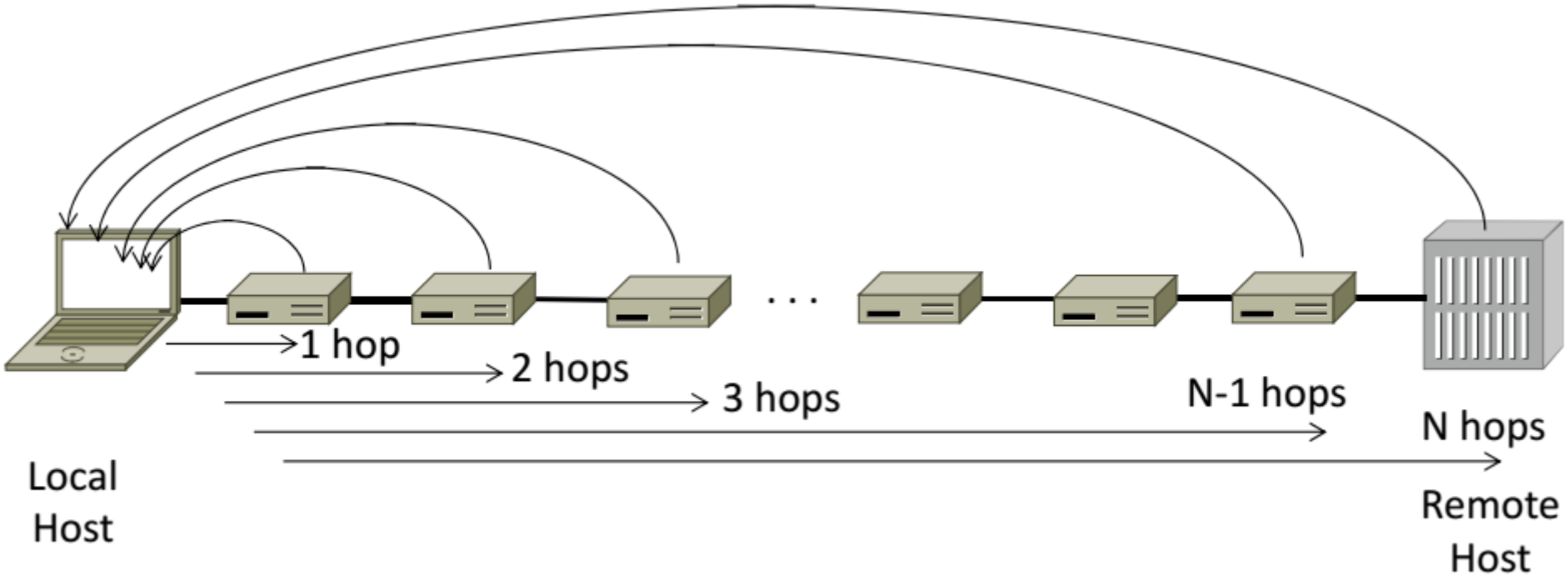
- به طور گسترده‌ای از ابزار خط فرمان (Command Line) استفاده می‌شود که به میزبانان (hosts) اجازه می‌دهد تا درون شبکه جستجو کنند.
  - روی تمام سیستم عامل‌ها (tracert on windows)
  - طراحی شده توسط Van Jacobson ~ 1987
  - استفاده از رابط شبکه - شبکه (IP) به نحوی که بعدا توضیح داده خواهدشد.

Traceroute (2)

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

میزبان محلی **میزبان راه دور**

Traceroute (3)



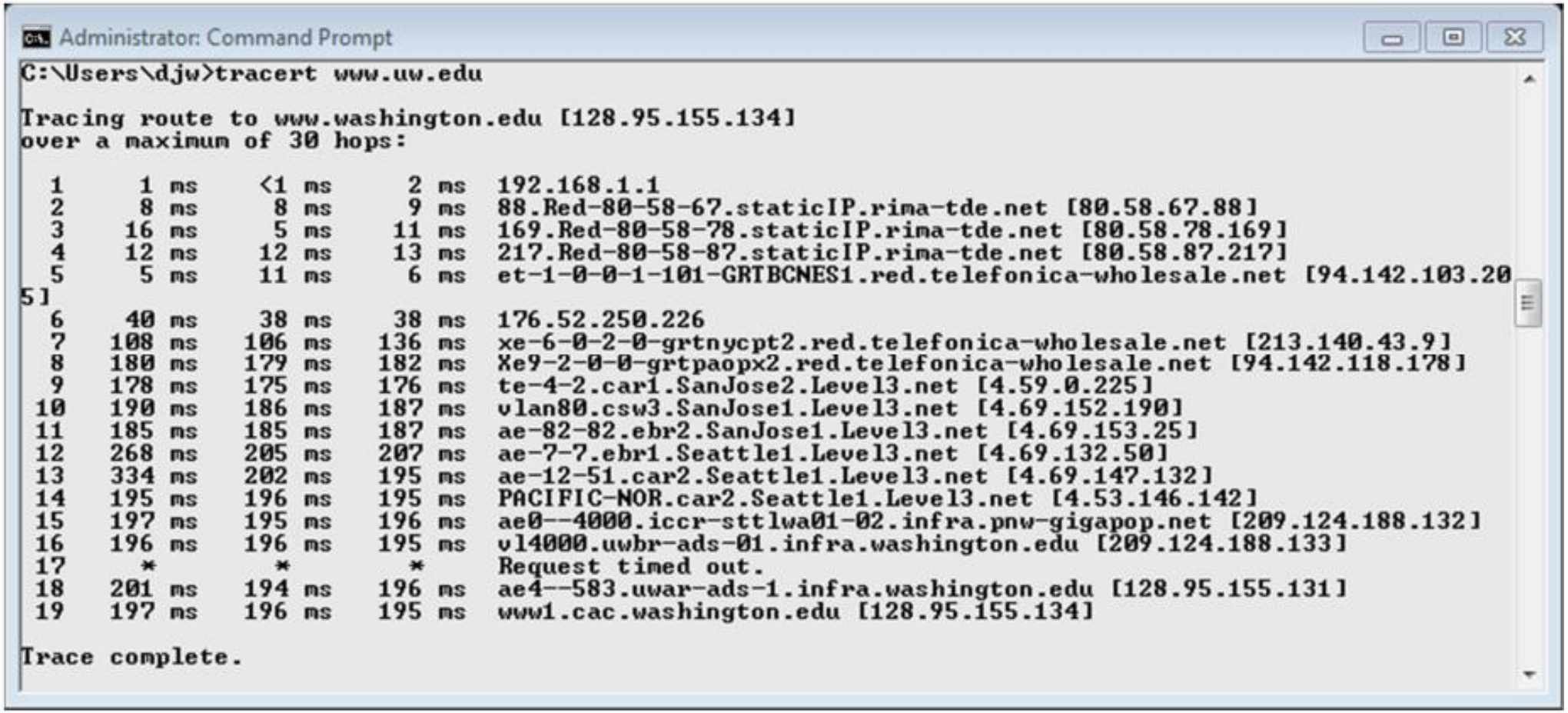
استفاده از Traceroute

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

مثال:

- Tracert www.uw.edu

استفاده از Traceroute



استفاده از Traceroute (۱)

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

Tracert برای هر هاپ ۳ بسته ارسال می‌کند 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 می‌گیرند.

استفاده از Traceroute (۲)

- چنانچه برای یک هاپ، بسته ارسالی دچار مشکل شود و به مبدا برنگردد، یک ستاره * بجای زمان، نمایش داده می‌شود.
- اولین هاپی که در خروجی Tracert قبل مشاهده می‌کنید، مودم ما با آی پی 192.168.1.1 می‌باشد. در صورتی که در یک LAN هستید و از طریق یک مودم به اینترنت متصل می‌شوید 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 می‌توان به آن اشاره کرد، IP های خصوصی هاپ‌ها است. این IP ها مربوط به روترهای شبکه اینترانت ISP و مخابرات می‌باشد.

استفاده از Traceroute (۳)

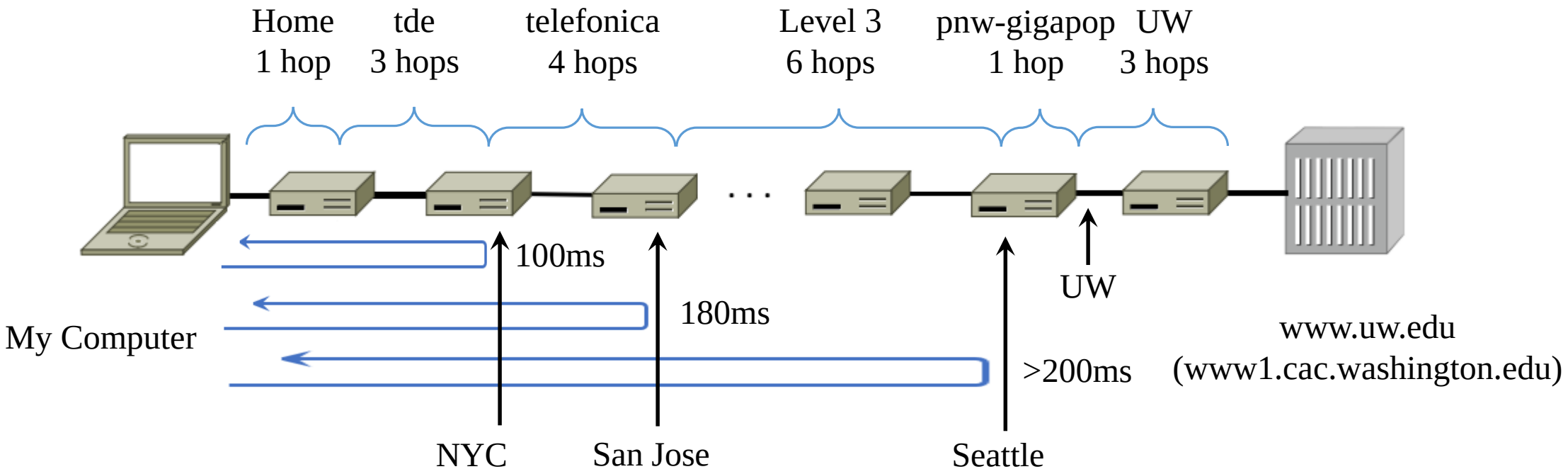
- با بررسی IP ها می‌توانیم شهرها و کشورهایی را که بسته‌های ما برای رسیدن به مقصد طی می‌کنند بیابیم.

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

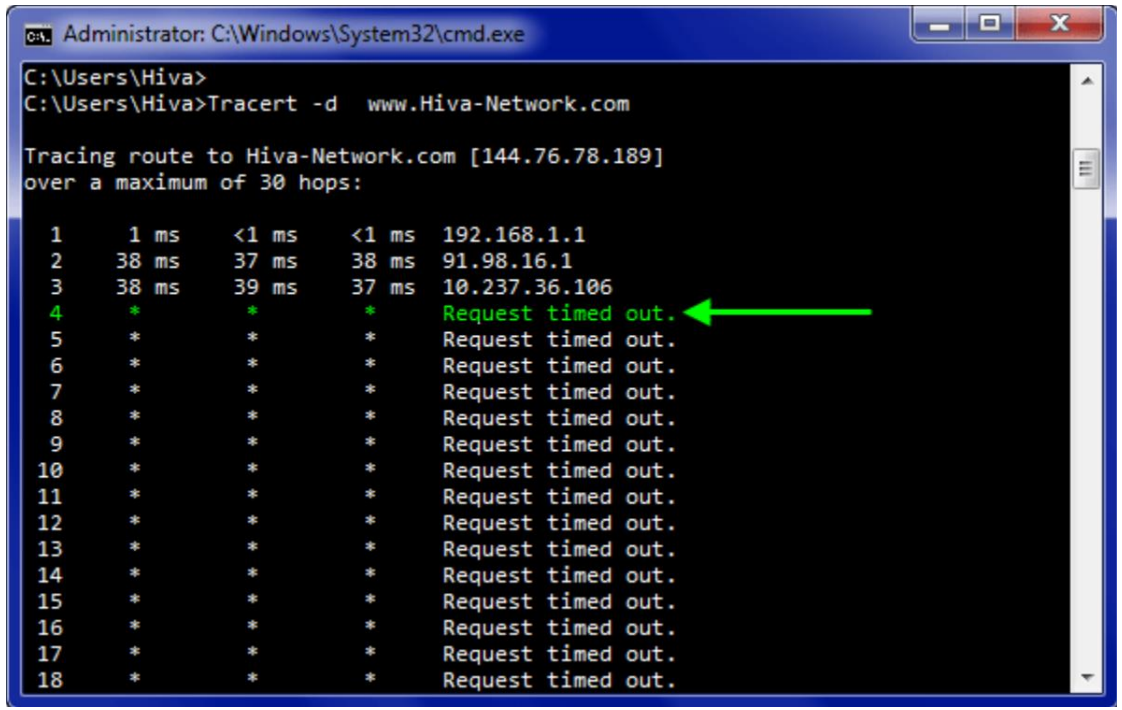
- **اگر در ارتباط بین بخش‌های مختلف اشکالی پیش بیاید چگونه با استفاده از دستور Traceroute آن را کشف کنیم؟**

حالت اول: فرض کنید شما دفتر نمایندگی شرکتی در اردبیل هستید. یک روز کاربران از سرعت پایین شبکه شاکی می‌شوند. شما می دانید که بسته‌های داده از شرکت شما مستقر در اردبیل تا دفتر مرکزی شرکت در تهران معمولا 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 معمولا 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.



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. کافیست یک بار بدون d– و یک بار با d– عمل Traceرا 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 پیش‌فرض تا ۳۰ هاپ نمایش داده خواهد شد.

سوئیچ‌های فرمان Traceroute

- **Tracert –w**

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

Tracert –w 100 www.uw.edu

در این مثال، حداکثر مدت زمان انتظار ۱۰۰ میلی ثانیه درنظر گرفته شده است.

مراجع این بخش

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