

آموزش رفع مشکلات ارتباطی شبکه به زبان ساده قسمت پنجم (نسخه PDF)

در ادامه سری مقالات رفع مشکلات ارتباطی شبکه به بررسی و تحلیل نتایج بدست آمده از دستور TRACERT می پردازیم . در مقاله قبلی از همین سری مقالات به شما آموزش دادیم که چگونه از دستور TRACERT برای پیدا کردن مشکلات ارتباطی شبکه بین کامپیوتر مبدا و سرور مقصد که ممکن است در شبکه ای خیلی خیلی دور قرار داشته باشد استفاده کنیم و بعد از آن روش ساده ای از نحوه استفاده از این دستور را به شما آموزش دادیم ، در این مقاله به شما آموزش می دهیم که چگونه نتایج حاصل از اجرای آن دستور را تحلیل کنید .

خوب برای اینکه راحت تر موضوع را درک کنید من قبلا دستور Tracert را برای مقصد www.espn.com اجرا کرده ام ، اگر می پرسید چرا این دامنه را انتخاب کرده اید به این دلیل است که مطمئن هستم این آدرس مقصد بسته های ICMP را بلوکه نمی کند و به آنها پاسخ می دهد . خوب در ادامه اجرای دستور فوق را با نتایج حاصل شده را مشاهده می کنید ، در تمام طول این مقاله از نتیجه این دستور استفاده می کنیم :

```
C:\Users\Administrator>TRACERT www.espn.com
Tracing route to www.espn.com [199.181.132.250] over a maximum of 30 hops:
  2 ms   1 ms   <1 ms  147.100.100.100
 10 ms  10 ms   9 ms  208.104.224.1
  9 ms   9 ms   9 ms  208.104.1.13
  9 ms   8 ms   9 ms  208.104.0.13
 10 ms   9 ms  10 ms  208.104.0.1
 11 ms  14 ms  10 ms  165.166.125.193
 11 ms  10 ms  11 ms  gig-1-1-3.core01.ncchrl.infoave.net [165.166.22.61]
 31 ms  31 ms  30 ms  64.200.130.17
 38 ms  39 ms  40 ms  hrndva1wxc2-pos15-3-oc48.wcg.net [64.200.240.213]
 31 ms  31 ms  31 ms  64.200.249.170
 31 ms  30 ms  31 ms  4.68.110.5
 48 ms  35 ms  35 ms  vlan99.csw4.Washington1.Level3.net [4.68.17.254]
 32 ms  31 ms  33 ms  ae-92-92.ebr2.Washington1.Level3.net [4.69.134.157]
 60 ms  53 ms  54 ms  ae-2.ebr3.Chicago1.Level3.net [4.69.132.69]
 86 ms  71 ms  70 ms  ae-3.ebr2.Denver1.Level3.net [4.69.132.61]
137 ms 103 ms 102 ms  ae-2.ebr2.Seattle1.Level3.net [4.69.132.53]
 95 ms  95 ms  95 ms  ae-23-52.car3.Seattle1.Level3.net [4.68.105.36]
 94 ms  95 ms  95 ms  WALT-DISNEY.car3.Seattle1.Level3.net [4.71.152.22]
 *      *      *      Request timed out.
 97 ms  95 ms  98 ms  199.181.132.250
Trace complete.
```

اگر به نتیجه دستور Tracert بالا نگاه کنید خواهید دید که در هر خط چندین نوع اطلاعات وجود دارد که نمایش داده شده است . اولین قسمت از نتایج بدست آمده در چپ ترین قسمت نتیجه عددی است که به شماره Hop متعلق است . همانطوری که قبلا هم گفتیم دستور Tracert بوسیله ارسال بسته های Ping به آدرس مقصد کار می کند . در هنگام صدور این دستور توسط سیستم عامل این دستور ابتدا بسته اطلاعاتی Ping را با ۱ TTL به اولین Hop ارسال میکند و اولین Hop این عدد ۱ را تبدیل به ۰ کرده و اطلاعات و نتیجه حاصل را به دستور باز می گرداند .

در ابتدا درخواست با TTL مقدار ۱ ارسال می شود و همین مسئله اطمینان حاصل می کند که در اولین Hop درخواست ارسال شده از بین

خواهد رفت . در این هنگام اطلاعات مربوط به آن Hop نمایش داده می شود و در ادامه بسته ICMP مجددا ارسال خواهد شد اما اینبار با مقدار ۲ ارسال میشود . این فرآیند کم و زیاد کردن و همچنین نمایش اطلاعات آنقدر ادامه می یابد تا اینکه بسته مورد نظر به مقصد برسد . در این هنگام دستور TRACERT به شما تعداد HOP ها و همچنین مسیری که بسته اطلاعاتی طی کرده است تا به مقصد مورد نظر برسد را نمایش خواهد داد .

اگر به آخرین خط نتایج بازگشت داده شده توسط دستور نگاه کنید عدد ۲۰ را مشاهده می کند که بدین معناست که ۲۰ عدد HOP در میان مبدا و مقصد وجود داشته است که بسته ما از این میان عبور کرده است و به مقصد رسیده است . سه قسمت دیگر موجود در ادامه هر خط از نتیجه ، مشخص کننده مقدار زمانی است که بسته برای رسیدن به هر یک از این روترها یا بهتر بگوییم HOP ها زمان برده است . اگر دقت کرده باشید در هر خط از این نتایج که ادامه پیدا کرده و از هر HOP عبور می کند به زمان آن هم اضافه می شود . همیشه دو نکته بسیار مهم است که در مورد زمان عبور بسته های بین HOP ها می بایست بدانید .

- اولین نکته : برای هر یک از HOP ها سه زمان مشخص و منحصر نمایش داده می شود . همانطوری که قبلا هم اشاره شد دستور Tracert بر مبنای ارسال درخواست های متعدد ICMP فعالیت می کند . در چند مقاله قبلی که با دستور Ping کار کردیم مشاهده کردید که دستور Ping همیشه با نمایش چهار مقدار برای اندازه گیری مقدار Packet Loss کار میکند . همین مفهوم در مورد دستور Tracert نیز صادق است با این تفاوت که تعداد زمانهایی که نمایش داده می شود ۳ است .

- دومین نکته : در صورتیکه زمان بازگشتی بصورت ستاره نمایش داده شود نشان دهنده این است که request timed out دریافت کرده ایم . این نوع پاسخ بسته به نوع ستاره ای که نمایش داده می شود ممکن است به دلیل وجود مشکل بوجد آمده باشد و یا اینکه مشکلی وجود ندارد . اگر شما به Hop شماره ۱۹ در تصویر بالا نگاه کنید می بینید که هر سه پاسخ ارائه داده شده بصورت ستاره نمایش داده شده است . زمانی که شما ۳ عدد ستاره پش سر هم در یک خط مشاهده کردید ، متوجه می شود که این HOP یک روتر یا یک فایروال است که پورت ICMP بر روی آن بلاک شده است و اجازه عبور ندارد و بنا بر همین اصل است که پاسخ را بصورت request timed ot دریافت خواهید کرد.

اما همیشه به خاطر داشته باشید که این لزوما نتیجه نهایی نیست و احتمالات دیگری نیز ممکن است وجود داشته باشد . Tracert زمانی که HOP در دسترس نباشد نیز سه عدد ستاره را به عنوان پاسخ نمایش خواهد داد . خوب در اینجا یک سؤال مهم پیش میاد که چگونه میتوانیم متوجه شویم که یک HOP پورتهای ICMP را بلاک کرده است و یا اینکه در دسترس نیست !!

این مسئله ممکن است کمی گمراه کننده باشد. در اینجا باید به این نکته جالب توجه داشته باشید که در صورتیکه لینک ارتباطی شما در دسترس نباشد و روتر دچار مشکل شده باشد در هر کجای مسیر که باشد پیام Trace Completed را دریافت خواهید کرد و تست به پایان می رسد. یک نشانه خوب برای اینکه متوجه شویم لینک ما قطع شده است وجود این است که در هر جایی که لینک ما قطع شده یا دچار مشکل می شود مابقی مسیر بصورت ستاره نمایش داده میشود و HOP های بعدی همگی نتایج ستاره ای نمایش می دهند و پیغام Request Timed Out را نمایش می دهند. برای مثال در قسمت پایین و در ادامه من وب سایت www.brienposey.com را با دستور Tracert تست می کنم و نتایج را نمایش می دهم:

```
C:\Users\Administrator>TRACERT www.brienposey.com
Tracing route to www.brienposey.com [24.235.10.4]
over a maximum of 30 hops:
 0 ms  0 ms  <1 ms  147.100.100.100
 8 ms  12 ms  8 ms  208.104.224.1
 9 ms  8 ms  9 ms  208.104.1.9
10 ms  9 ms  8 ms  208.104.0.9
10 ms  12 ms  11 ms  208.104.0.5
12 ms  10 ms  9 ms  165.166.18.1
15 ms  23 ms  13 ms  gig2-2-1.c01.scclma.infoave.net [165.166.22.17]
13 ms  12 ms  13 ms  66.192.166.9
31 ms  30 ms  *  peer-01-ge-0-0-0-1.asbn.twtelecom.net [64.129.249.10]
56 ms  57 ms  55 ms  hb0-0-0-0.in.telia.aberlabele.net [151.164.242.50]
```

```

56 ms  57 ms  55 ms  dd2-pb-u.ipltin.sbcglobal.net [151.164.242.59]
55 ms  53 ms  55 ms  ded2-g8-0.ipltin.sbcglobal.net [151.164.42.159]
59 ms  56 ms  56 ms  Winnet-1148485.cust-rtr.ameritech.net [66.73.221.254]
64 ms  63 ms  68 ms  216-24-2-237.ip.win.net [216.24.2.237]
68 ms  68 ms  64 ms  fa0-0.cust-gw2.noc.win.net [216.24.30.69]
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
* * * Request timed out.
Trace complete.

```

اگر نتایج بالا را مشاهده کنید قطعی لینک را به وضوح مشاهده خواهید کرد اما این بصورت قطعی پاسخ مشکل ما نخواهد بود . بهترین نتیجه از این دستور این است که چندین مقصد مختلف را با دستور آزمایش کنیم و نتایج حاصل را با هم مقایسه کنیم . همیشه در نظر داشته باشید که تعداد زیاد HOP نشان دهنده این است که مقصد از شما فاصله زیادتری دارد و هرچقدر هم این مسیر از ما دورتر باشد رفع ایراد آن دشوار تر خواهد بود .

در صورتیکه شما از مسیره‌های مختلف و از سایت‌های مختلف مسیر را تست کنید بهترین نتیجه ممکن را در خصوص قطعی لینک بدست خواهید آورد. آخرین قسمت هر خط از پاسخی که توسط دستور Tracer نمایش داده می شود نام مسیریابی است که به درخواست ICMP فرستاده شده پاسخ داده است. دستور Tracert تا حد امکان سعی می کند که نام روتر را به شما نمایش دهد اما در بسیاری از مواقع این امر امکانپذیر نیست . برای مثال اگر به نتایج بالا دقت کنید خواهید دید که بیش از نیمی از روترها با نام مشخص شده اند و این در حالی است که بقیه آنها با نام مشخص نشده اند. البته این چندان اهمیتی در اصل موضوع رفع ایراد ندارد.

نکته جالب این است که ممکن است میزبان یا همان هاستی که شما برای آن تست را انجام می دهید همیشه شناسایی نشود !!! برای مثال در اولین تستی که در همین مقاله با دستور Tracert انجام دادیم و با زدن دستور Tracert www.espn.com انجام شد بلافاصله دستور Tracert آدرس IP به شماره ۱۹۹.۱۸۱.۱۳۲.۲۵۰ را بازگرداند. اگر شما آخر نتیجه دستور مثال بالا را نادیده بگیرید خواهید دید که دستور Tracert در نهایت به مقصد خواهد رسید اما مقصد را معملا با نام نمایش نخواهد داد (حداقل در مثال ما) . این رفتار یک مشکل نیست بلکه یک طراحی است . دلیل اینکه من برای شما مثال بالا را بکار بردم ای است که شما معملا دستور Tracert را برای یک وب سایت بکار نمی برید و البته من فکر میکنم که در مثال بالا به دلیل این نتایج به مشکل خورد که ما با نام مقصد را تعیین کردیم و نه با آدرس IP مقصد.

- نتیجه :** در این مقاله به شما نحوه تجزیه و تحلیل نتایج حاصل از دستور Tracert را به شما آموزش دادم ، در مقاله بعدی به شما نحوه استفاده از دستور Route را آموزش خواهم داد و اینکه چگونه می توانید Routing Table کامپیوتر را آزمایش کنید و آن را تغییر

دهید. ITPRO باشید

هرگونه نشر و کپی برداری بدون ذکر منبع و نام نویسنده دارای اشکال اخلاقی می باشد

فرهاد خانلری

امیدوارم مثل همیشه سرشمار از انرژری باشی...
برات بهترین ها رو آرزومندم.

محسن خدابنده اوپلی

سلام ممنون مهندس جان
مقاله بعدیش کی میاد مهندس
در مورد روت rout
در انتها نوشته بودید

فواد باوی

مرسی از لطفتون مهندس جان
پیروز باشید

farid۱۳۶۶

سلام خیلی خیلی ممنونم برای زحماتی که می کشید من ۵ قسمت مقاله های شما را خواندم بسیار عالی بودند طی فرمایشات شما من متوجه شدم که DNS کامپیوترم تایم اوت دارد چند تا دیگه امتحان کردم که مشکل تایم اوت نداشتن ولی مشکلم رو حل نکردن در بازی آنلاین دچار گیر و پرش فراوان و قطعی هستم اگر ممکن هست راهنمایی کنید که چه کار کنم مشکلم حل شود در ضمن من دستور Tracert اجرا کردم با DNS و این نتیجه حاصل شد

□

اگر زحمت بکشید و راهنمایی بفرمایید بسیار سپاسگزار هستم

davood_۵۹

سلام آقای مهندس؛

مقاله بسیار جالب و خوبی بود. فقط در زمینه خطایابی و برای اینکه زودتر به خطا برسیم، مرحله به مرحله جلو میریم تا اینکه به محل اصلی خطا برسیم. حالا بطور مثال با دو پیغام تو این زمینه مواجه میشیم. الان کدوم یکی یک گام به حل مسئله برای ما نزدیکتر هستش؟

(الف)

request timed out

(ب)

.Ping: transmit failed. General failure

فکر کنم الف بهتر باشه و به حل خطا نزدیکتر شدیم. درست میگم؟

محمد نصیری

الف بیشتر به خاطر جلوگیری از رد شدن بسته هست مثلا- فایروال ... دومی به خاطر تنظیمات اشتباه IP و خطاهای فیزیکی و پیکربندی هست بیشتر

davood_۵۹

خیلی خیلی ممنون و متشکرم آقای مهندس. دست گلتون درد نکنه.

خوب آقای نصیری پیغام :

Destination Host Unreachable

هم مثل مورد ب هستش . درست میگم خدمتون؟

میخوام این رو درک کنم که اگه بخوایم گام به گام به رفع خطا نزدیکتر بشیم، کدوم یکیشون نشون دهنده این هستش که داریم به حل خطا می رسیم؟ فکر کنم request timed out نسبت به بقیه نشوندهنده وجود خطاهای کمتر و نزدیکتر شدن به حل مشکلمون هستش. درست میگم خدمتون؟

ببخشید اگه ممکنه سوالم خیلی جالب و یا از نظر فنی درست نباشه. عذرخواهم ازتون.

مطلب اصلی