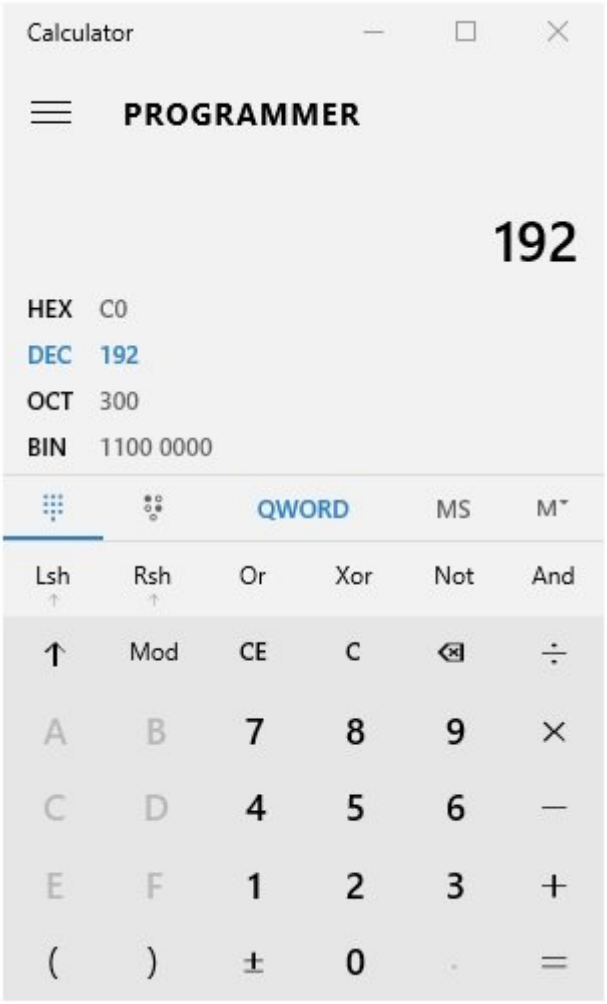
فرآیند محاسبه آدرس های IPv6 و آشنایی با چند ابزار نظارت بر شبکه‌های مبتنی بر ویندوز سرور 2019

اطلاع پیدا کردیم که بخش‌های مختلف یک آدرس برای چه مقاصدی استفاده می‌شوند. اکنون اجازه دهید درباره نحوه چگونگی اختصاص شماره‌های شناسه منفرد به تمامی کامپیوترها، سرورها و سایر دستگاه‌های موجود در شبکه اطلاعاتی به دست آوریم.

برای مطالعه قسمت قبل **آموزش رایگان ویندوز سرور 2019** اینجا کلیک کنید.

شما می‌توانید کار را با شماره 1 شروع کرده و این‌کار را ادامه دهید. ایده دیگر این است که آدرس‌های IPv4 قدیمی را در قالب هگزا محاسبه کرده و از آن‌ها به عنوان 32 بیت آخر یک آدرس استفاده کنیم. ماشین حساب ویندوز را باز کرده، روی منو کلیک کرده و حالت ماشین حساب را Programmer تعیین کنید. ماشین حساب ویندوز یک ابزار سریع و آسان است که می‌توانید برای تبدیل مقادیر دهگان به هگزا از آن استفاده کنید. اجازه دهید به مثال وب‌سرور که در حال اجرا است و از آدرس با 192.168.1.5 استفاده می‌کند مراجعه کنیم. من می‌خواهم IPv6 را درون شبکه خود پیاده‌سازی کنم و می‌خواهم آدرس‌های IPv6 سرور من آدرس IPv4 اصلی را در بخش شناسه دستگاه آدرس جدید منعکس کنند. در ماشین حساب، مقدار 192 را تایپ می‌کنم و سپس روی HEX کلیک می‌کنم. همان‌گونه که در شکل زیر نشان داده شده، مقدار هگزاعدد 192 محاسبه شده و نشان داده می‌شود:



اگر این‌کار را با هر سایر اوکت‌های آدرس IPv4 انجام دهید نتیجه زیر را دریافت می‌کنید:

```
192 = C0
168 = A8
1 = 01
5 = 05
```

بنابراین معادل آدرس 192.168.1.5 در IPv6 برابر با C0A8: 0105 می‌شود. اکنون می‌توانیم از این ترکیب در تعامل با پیشوند سازمانی و شناسه زیرشبکه خود برای ایجاد یک آدرس IPv6 ایستا برای وب‌سرور وب استفاده کنیم.

2001:AABB:CCDD:0001:0000:0000:C0A8:0105

در آدرس قبلی IPv6 متوجه شدید که من مقدار هگزا را به انتهای شناسه دستگاه اضافه کردم و همچنین تغییرات دیگری را نیز اعمال کردم. از آن‌جایی که ما 64 بیت آخر را برای شناسه دستگاه در اختیار داریم، اما آدرس قدیمی IPv4 ما فقط 32 بیت مصرف می‌کند، من 32 بیت در وسط قرار دارم. این کار عجیب به نظر می‌رسد که داده‌هایی در این‌جا داشته باشیم که معنایی برای ما نداشته باشند. بنابراین برای ساده کردن آدرس همه آن‌ها را صفر می‌کنیم وعلاوه بر آن شناسه زیر شبکه خود را به شماره 1 تغییر و تنظیم می‌کنیم، زیرا این اولین زیر شبکه در شبکه ما است.

آدرس جدید ما کمی بهتر شده و مفهوم دقیق‌تری پیدا کرده است. اکنون که آدرس جدید برای وب‌سرور مشخص شده است باید یکسری کارهای دیگر هم انجام دهیم تا آدرس ما بازهم دقیق‌تر شود. در حال حاضر آدرس ما کاملا دقیق است. من می‌توانم این آدرس آی‌پی را به خصوصیات کارت شبکه وب‌سرور متصل کنم تا بدون مشکل کار کند. با این حال، تعداد زیادی صفر در آدرس من وجود دارد و لازم نیست که من همه آن‌ها را حفظ کنم. هر زمان که صفرهای غیر ضروری در یک بخش 16 بیتی داشتید که متجاوز از تعداد واقعی آن‌ها است به سادگی می‌توانید آن‌ها را حذف کنید. به عنوان مثال، شناسه زیر شبکه ما و 32 بیت اول شناسه دستگاه ما صفرهای غیر ضروری زیادی دارند، بنابراین می‌توانیم آدرس را به شرح زیر خلاصه کنیم:

2001:AABB:CCDD:1:0:0:C0A8:0105

حتا این امکان وجود دارد که بازهم یک قدم روبه جلو برداریم و هر زمان که بخش‌های کامل 16 بیتی داشتیم که کاملا از صفرها تشکیل شده است از دو کاراکتر دو نقطه به جای آن‌که آن‌ها استفاده کنیم. بنابراین، 32 بیت اول شناسه دستگاه من که همه صفر هستند را می‌توان با دو کاراکتر کولون (::) جایگزین کرد. در زیر آدرس کامل و آدرس تلفیقی را مشاهده می‌کنید. این اعداد کاملاً متفاوت به نظر می‌رسند. آدرس تلفیقی بسیار ساده است، اما از دیدگاه فناوری دقیقاً هر دو آدرس یکسان هستند.

2001:AABB:CCDD:0001:0000:0000:C0A8:0105
2001:AABB:CCDD:1::C0A8:0105

در واقع، اگر محیطی را آماده کنید یا می‌خواهید IPv6 را به سرعت آزمایش کنید، به سادگی می‌توانید از آدرس‌های تلفیقی استفاده کنید. هر دو آدرس زیر یکسان هستند:

2001:0000:0000:0000:0000:0000:0000:0001
2001::1

با اطلاعاتی که به دست آوردید، باید بتوانید یک آدرس IPv6 را ایجاد کرده و در زیرساخت‌هایی که از IPv6 پشتیبانی می‌کنند از آدرس‌های مبتنی بر این پروتکل برای سرویس‌دهی به کامپیوترها یا سرورهای شبکه استفاده کنید. نکات زیاد دیگری نیز در مورد IPv6 وجود دارند که خود به تنهایی یک کتاب کامل می‌شوند.

جعبه ابزار شبکه

این‌که یک مدیر سرور، یک مدیر شبکه یا ترکیبی از هر دو حالت هستید، تفاوتی ایجاد نمی‌کند. یک کارشناس شبکه به ابزارهای مختلفی برای آزمایش و نظارت بر ارتباطات شبکه در دنیای ویندوز سرور نیاز دارد. برخی از این ابزارها در خود سیستم‌عامل قرار دارند و از طری خط فرمان و پاورشل قابل استفاده هستند و برخی دیگر رابط‌های گرافیکی گسترده‌تری دارند که پیش از استفاده باید نصب شود. در ادامه به ابزارهای پر کاربرد زیر در شبکه نگاهی خواهیم داشت

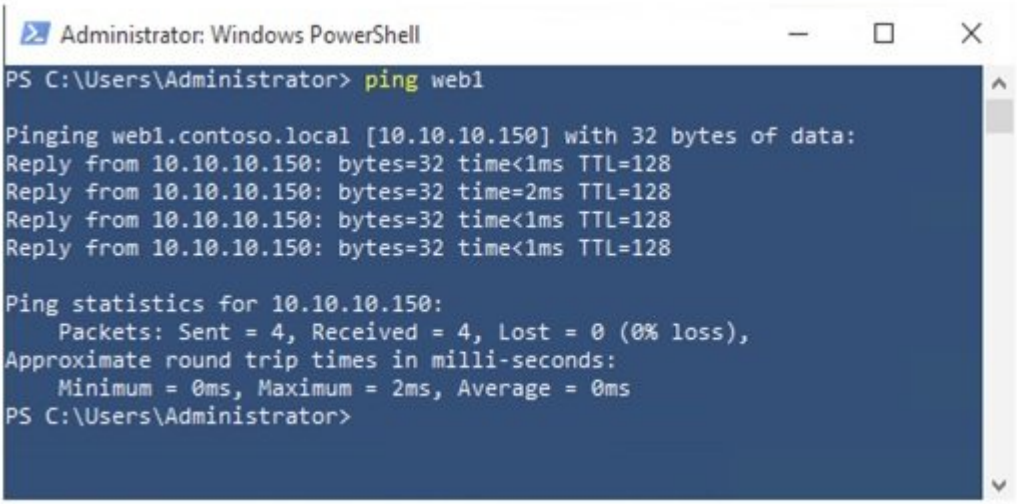
- ping
- tracert
- pathping
- Test-Connection
- telnet
- Test-NetConnection

تمامی این ابزارها رایگان هستند و بنابراین هیچ بهانه‌ای برای عدم آشنایی با این ابزارها وجود ندارد.

Ping

هر متخصص شبکه‌ای باید اطلاعات کافی درباره ابزار Ping داشته باشد. ping دستوری است که می‌توانید از طریق خط فرمان یا پاورشل از آن استفاده کنید و اطلاعاتی درباره DNS یا یک آدرس آی‌پی به دست آورید. پینگ یکی از پر کاربردترین ابزارهای شبکه است که برای بررسی وضعیت اتصال دو دستگاه در یک شبکه از آن استفاده می‌شود.

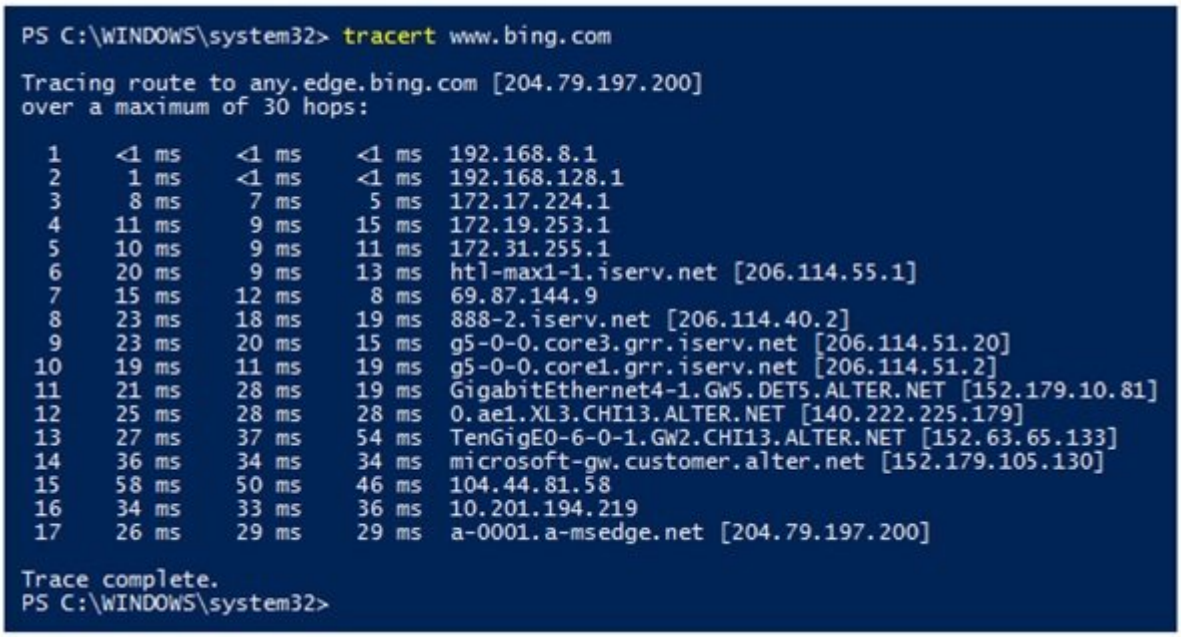
از طریق سرویس‌گیرنده ویندوز 10 در یک شبکه محلی، می‌توان خط فرمان را باز کرده و یک پینگ به <IP_ADDRESS> انجام دهیم. از طرف دیگر، اگر در محیط کاری از DNS استفاده می‌کنید که نام‌ها را به آدرس‌های آی‌پی تبدیل می‌کند، این امکان وجود دارد که از ترکیب نحوی <ping <SERVERNAME استفاده کنیم، همان‌گونه که در مثال زیر نشان داده شده است. در این حالت سرور به پینگ ما واکنش نشان می‌دهد و اجازه می‌دهد مطمئن شویم که در وضعیت آنلاین قرار دارد.



ترافیک پینگ از لحاظ فنی ترافیک ICMP نامیده می‌شود. این موضوع مهم است، زیرا این روزها و به‌طور پیش‌فرض ICMP در حال مسدود شدن است و در بسیاری از سیستم‌ها و دستگاه‌های ما دیوارهای آتش روشن فرآیند ارسال و تبادل اطلاعات روی ICMP را مسدود می‌کنند. به لحاظ تاریخی، پینگ همواره ابزاری است که می‌توانیم از آن برای بررسی وضعیت اتصال دو دستگاه و اطلاع درباره قطعی یک اتصال از آن استفاده کنیم. اما همیشه این‌گونه نیست.
در برخی موارد ممکن است یک کامپیوتر ویندوزی را پیکربندی کنید و به شبکه متصل کنید و کامپیوتر با اینترنت و همه سرورهای موجود در شبکه شما ارتباط برقرار کند، اما اگر سعی کنید به کامپیوتر جدید از دستگاه دیگری در شبکه پینگ کنید، پینگ عدم وجود اتصال را نشان دهد. چرا این اتفاق می‌افتد؟ از آن‌جایی که ویندوز به‌طور پیش‌فرض یکسری کارهای امنیتی انجام می‌دهد که مسدود کردن ترافیک ICMP در دیوارآتش ویندوز از جمله این موارد است.
در این حالت، باید دیوارآتش را خاموش کنید یا یک قاعده دسترسی را تعریف کنید که امکان تبادل ترافیک از طریق ICMP را فراهم کند. پس از فعال شدن چنین قاعده‌ای، پینگ وضعیت درست اتصال به کامپیوتر جدید را نشان می‌دهد. هر زمان سیستم‌ها یا سرورهای جدیدی در شبکه خود ایجاد کردید به خاطر داشته باشید که پینگ همیشه قابل اعتمادترین ابزار دنیای شبکه برای بررسی وضعیت اتصالات است.
با اضافه کردن یک قاعده به دیوارآتش ویندوز دیفندر از طریق بخش Advanced Security می‌توانید پاسخ‌های ICMP را دریافت کنید. خوشبختانه، در حال حاضر می‌دانید که چگونه می‌توانید از Group Policy به منظور ایجاد GPO استفاده کنید و آن‌را روی تمام دستگاه‌های موجود در شبکه خود اعمال کنید. همچنین، این امکان وجود دارد که قواعد دیوارآتش را به‌طور کامل در GPO قرار دهید. این یک روش معمول برای اجازه دادن یا مسدود کردن ICMP در کل شبکه یک سازمان است که یک قاعده دیوارآتش را از طریق Group Policy اعمال کنید.

Tracert

tracert که کوتاه شده Trace Route است، ابزاری است که برای ردیابی بسته‌های شبکه در هنگام گذر از شبکه استفاده می‌شود. کاری که ابزار فوق انجام می‌دهد این است که تمامی مکان‌هایی که بسته‌ها به آن مکان‌ها می‌روند را پیش از رسیدن به مقصد مشاهده می‌کند. مکان‌هایی که بسته‌ها پیش از رسیدن به مقصد از میان آن‌ها در یک شبکه عبور می‌کنند هاپ نامیده می‌شود. ابزار Trace تمامی هاپ‌هایی را که ترافیک شما هنگام حرکت به سمت سرور مقصد از آن‌ها عبور کرده یا با آن‌ها در تماس است را نشان می‌دهد. اگر پنجره پاورشل را از یک دستگاه متصل به اینترنت باز کنیم و از ابزار Tracert در ارتباط با یک وب‌سرویس شبیه به Bing استفاده کنیم نتایج جالبی را به دست می‌آوریم.



این اطلاعات به ویژه زمانی که سعی در تشخیص ارتباطی دارید که به درستی کار نمی‌کند مفید هستند. اگر ترافیک شما قبل از رسیدن به مقصد از طریق چندین هاپ مانند روتر و دیوارآتش عبور می‌کند، ردیابی می‌تواند در تشخیص اینکه در هر مکان چه اتفاقاتی رخ داده است حائز اهمیت می‌شود. با توجه به اینکه عکس قبلی مسیر موفقی به Bing را نشان می‌دهد، حالا بیایید ببینیم که وقتی ارتباطی با شکست روبرو می‌شود، چه اتفاقی رخ می‌دهد. من روتر خودم را از اینترنت جدا می‌کنم و دوباره همان ردیابی به سایت www.bing.com را اجرا می‌کنم. اکنون می‌توانیم مشاهده کنیم که من هنوز هم می‌توانم با روتر محلی خودم ارتباط برقرار کنم، اما کار بیشتری نمی‌توانم انجام دهم.

Pathping

tracert مفید است و به نظر می‌رسد ابزار استانداردی برای ردیابی بسته‌های مرتبط با شبکه شما است، اما به نظر من دستور Pathping قدرتمندتر است. pathping دقیقاً همان کار ردیابی را انجام می‌دهد به جز این‌که اطلاعات مهم دیگری نیز ارائه می‌کند. بیشتر اوقات، با هر یک از این دستورات شما به دنبال بررسی این موضوع هستید که در زنجیره هاپ‌ها شکستی رخ نداده باشد، اما در بیشتر موارد ما سرورها را برای شبکه‌سازی پیکربندی می‌کنیم و با سخت‌افزارها، سرورها و کارت‌های شبکه مختلفی کار می‌کنیم. هنگام کار با چند کارت شبکه در یک سیستم جدول مسیریابی محلی به همان اندازه روترها و سوییچ‌های خارجی حائز اهمیت می‌شود و مجبور هستیم در بیشتر موارد مسیر یک بسته شبکه و کارت شبکه را بررسی می‌کنیم. این همان مکان یاست که pathping به عنوان ابزاری قدرتمندتر از tracert به میدان وارد می‌شود. اولین بخش از اطلاعاتی که tracert به شما نشان می‌دهد اولین هاپ از سرور محلی است که در حال گذر از آن هستید، اما pathping به شما نشان می‌دهد کدام رابط شبکه محلی در حال انتقال بسته‌ها است.

```
PS C:\Users\jkrause> pathping www.bing.com

Tracing route to any.edge.bing.com [204.79.197.200]
over a maximum of 30 hops:
  0  IVO-PC-328 [192.168.8.113]
  1  192.168.8.1
  2  192.168.128.1
  3     *     192.168.8.1  reports: Destination host unreachable.

Computing statistics for 75 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           IVO-PC-328 [192.168.8.113]
                                    0/ 100 =  0%   |
  1    1ms     0/ 100 =  0%     0/ 100 =  0%  192.168.8.1
                                  100/ 100 =100%   |
  2  ---     100/ 100 =100%     0/ 100 =  0%  192.168.128.1
                                    0/ 100 =  0%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  IVO-PC-328 [0.0.0.0]

Trace complete.
PS C:\Users\jkrause>
```

اجازه دهید برای روشن شدن مطلب مثالی بزنیم. من اغلب سرورهای دسترسی از راه دور را با چند کارت شبکه تنظیم می‌کنم و در طی این فرآیند مسیرهای بسیاری را روی سرور محلی ایجاد می‌کنیم تا سرور راه دور بداند چه ترافیکی نیاز به ارسال دارد و ترافیک باید در چه جهتی اتقال پیدا کند. چه ترافیکی باید از کارت شبکه داخلی و چه ترافیکی باید از طریق کارت شبکه خارجی انتقال پیدا کند. پس از کامل شدن تمامی دستورات مسیریابی برای کارت شبکه داخلی، ما دستورات را آزمایش می‌کنیم و یک پینگ روی سرور داخل شبکه انجام می‌دهیم. شاید این پینگ شکست بخورد و ما به درستی دلیل این شکست ار متوجه نشویم. من می‌توانم یک دستورالعمل tracert را آزمایش کنیم، اما اطلاعات مفیدی به دست نخواهم آورد، زیرا نمی‌تواند اولین هاپ را مشاهده کند و پیغام time out را نشان می‌دهد. با این حال، اگر از دستور pathping استفاده کنم، اولین هاپ هنوز هم time out را نشان می‌دهد، اما اکنون می‌توانم ببینم که ترافیک من در تلاش است تا از کارت شبکه خارجی خارج شود. این مسئله نشان می‌دهد که پیکربندی ما روی مسیر ایستا در این سرور مشکلی دارد. بنابراین می‌دانیم که باید آن مسیر را حذف کرده و مسیر را از نو ایجاد کنیم تا ترافیک از طریق کارت شبکه داخلی عبور کند.

در تصویر زیر پنجره پاورشلی را مشاهده می‌کنید که نتیجه اجرای فرمان pathping را نشان می‌دهد. مشاهده می‌کنید که فرمان pathping یک آدرس آی‌پی محلی را روی لپ‌تاپ من نشان می‌دهد که تلاش می‌کند ترافیک به خارج از سیستم هدایت کند، در حالی که دستور tracert این اطلاعات را نشان نمی‌دهد:

```
PS C:\Users\jkrause> pathping www.bing.com

Tracing route to any.edge.bing.com [204.79.197.200]
over a maximum of 30 hops:
  0  IVO-PC-328 [192.168.8.113]
  1  192.168.8.1
  2  192.168.128.1
  3     *     192.168.8.1  reports: Destination host unreachable.

Computing statistics for 75 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           IVO-PC-328 [192.168.8.113]
                                    0/ 100 =  0%   |
  1    1ms     0/ 100 =  0%     0/ 100 =  0%  192.168.8.1
                                  100/ 100 =100%   |
  2  ---     100/ 100 =100%     0/ 100 =  0%  192.168.128.1
                                    0/ 100 =  0%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  IVO-PC-328 [0.0.0.0]

Trace complete.
PS C:\Users\jkrause>
```

در شماره آینده آموزش رایگان **ویندوز سرور 2019** مبحث فوق را ادامه خواهیم رفت.

تاریخ انتشار:
01 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16045/%D9%81%D8%B1%D8%A2%DB%8C%D9%86%D8%AF-%D9%85%D8%AD%D8%A7%D8%B3%D8%A8%D9%87-%D8%A2%D8%AF%D8%B1%D8%B3-%D9%87%D8%A7%DB%8C-ipv6-%D9%88-%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%DA%86%D9%86%D8%AF-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1-%D9%86%D8%B8%D8%A7%D8%B1%D8%AA-%D8%A8%D8%B1-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C