دستورPing

Ping اصلی ترین دستورTCP/IP برای عیب یابی اتصال – در دسترس بودن و ترجمه اسامی Name) (resolutionمیباشد.در واقع می تواند نقطه شروع مناسبی برای اشکال زدائی یک شبکه مبتنی بر **TCP/IP** باشد .بیشتر مدیران شبکه با این دستور کاملا آشنا هستند و تقریبا هرروز از آن استفاده می کنند . ساده ترین کاربرد این دستوربرای تست وضعیت ارتباط بین دو سیستم موجود درشبکه می باشد و همچنین مدت زمان ارسال و دریافت بسته اطلاعاتی نیز برآورد می شود. برنامه Ping درابتدا توسط **Mike Muuss**و با عملکردی ساده ، پیاده سازی گردید این برنامه از پروتکل **ICMP**اقتباس شده از Internet) (Control Message Protocolبه منظورمبادله بسته ها ی اطلاعاتی با سیستم راه دور به یک آدرس **ECHO**) (**REQUEST**و از پروتکل **UDP**برای حمل داده استفاده می نماید.

پس از ارسال پیام ، در انتظار دریافت پاسخ (**ECHO REPLY**) می ماند . سیستم راه دور، یک بسته اطلاعاتی از نوع پاسخ (REPLY)را برای فرستنده پیام ارسال می نماید و براساس آن Round-trip (ارسال یک درخواست و دریافت پاسخ محاسبه می گردد). ساختار بسته های اطلاعاتی **ECHO REQUEST** و **ECHO REPLY**درجدول زیرنشان داده شده است . از فیلد اطلاعاتی "نوع پیام" به منظور مشخص نمودن نوع پیام ، استفاده می شود . درصورتی که مقدار این فیلد هشت باشد ، بسته اطلاعاتی از نوع ECHO REQUEST و در صورتی که مقدار این فیلد صفر باشد ، بسته اطلاعاتی از نوع ECHO REPLY خواهد بود.

استفاده ازPing

Pingدارای عملکردی بسیارساده است . در ابتدا فیلد Sequence number مقدارصفررا خواهد گرفت و به ازای ارسال هر بسته اطلاعاتی، یک واحد به آن اضافه می شود . مقدار فیلد Identifierمنحصربفرد بوده تا امکان تشخیص بسته های اطلاعاتی برگردانده شده وجودداشته باشد (درمواردی که بیش از یک کاربر بطور همزمان از دستور Ping برروی یک ماشین استفاده می نمایند) در اکثرنسخه های یونیکس و لینوکس، مقدار فیلد Identifierمعادل Process ID پردازه ای در نظر گرفته می شود که پیام ECHO REQUEST را ارسال نموده است .

پس از دریافت پیام ECHO REQUEST توسط کامپیوتر دریافت کننده ، وی یک پاسخ (**REPLY**) را برای فرستنده ارسال می نماید که شامل Identifier و Sequence number مشابه بسته اطلاعاتی ارسالی است.

با توجه به پاسخ ارائه شده توسط دریافت کننده بسته های اطلاعاتی می توان به نتایج متفاوتی دست یا فت: تمامی بسته های اطلاعاتی ارسالی ، مجددا" برگردانده می شوند . (بین سیستم ارسال کننده و دریافت کننده مشکل ارتباطی وجود ندارد . برخی ازبسته های اطلاعاتی ارسالی ، توسط دریافت کننده برگرداند ه نمی شوند (کاهش بسته های اطلاعاتی ارسالی) و یا با اولویتی که ارسال می گردند با همان اولویت دریافت نمی شوند . این مسئله می تواند نشان دهنده وجود اشکال در یک شبکه باشد.
در این رابطه احتمال دیگری نیز وجود دارد:

سیستم از راه دور (سیستمی که می بایست به پیام های ارسالی پاسخ دهد) درگیر پردازش های متعددی است وقادربه پاسخگوئی پیام های ECHO REQUESTدرمدت زمان مشخص شده نمیباشد . دستور Ping مدت زمان Round-trip بر حسب میلی ثانیه را محاسبه و نما یش می دهد . برای محاسبه مدت زمان **Round-trip**برنامه ping زمان ارسال بسته اطلاعاتی را در فیلد **Optional data**قرار داده و پس ازبرگشت بسته اطلاعاتی، زمان ذخیره شده را با زمان جاری سیستم مقایسه نموده تا در نهایت مدت زمان رفت برگشت یک بسته اطلاعاتی مشخص گردد . دستور Ping همچنین مقدار TTL اقتباس شده از(Time To Live) را در خروجی

نمایش خواهد داد .TTL مدت زمان اعتبار یک بسته اطلاعاتی را مشخص نموده و هر host و یا روترموجوددر مسیر بسته اطلاعاتی معمولا" به میزان یک ثانیه آن را کاهش می دهد . در برخی موارد ممکن است درزمان ارسال درخواست های متوالی ping،مدت زمان Round-tripکاهش پیدا نماید .این موضوع می تواند دلایل متعددی داشته باشد:

ماشین مقصد و یا روتر (gateway) درآن مقطع زمانی درجدول محلی ARP نمی باشد ومدت زمانی طول خواهد کشید(میلی ثانیه) تا arp آدرس سخت افزاری اولین بسته اطللاعاتی را بدست آورد. در صورتی که به همراه دستور ping درمقابل استفاده از آدرس IP از نام host استفاده شود ، ممکن است یافتن سرویس دهنده DNS که برنامهping می بایست با آن ارتباط برقرار نماید(ترجمه نام host به آدرس) IPزمان خاص خودراداشته باشد.
در زمان استفاده از دستور Ping بهتر است که درابتدا عملیات ping را در ارتباط با اینترفیس محلی و یا آدرس **ip** : **Loopback 127.0.0.1**شروع نمود .آدرس **Loopback**در پشته TCP/IP استفاده شده و می توان از آن به منظورحصول اطمینان ازصحت کارکرد پشته محلی،استفاده نمود. آدرس فوق یک آدرس IP رزرو شده است که امکان استفاده ازآن دراینترنت وجود ندارد درصورتی که نمی توان آدرسIPسیستم محلی را ping نمود، ممکن است پیکربندی سیستم دارای مشکل باشد در صورتی که نمی توان آدرس **Loopback**را ping نمود ممکن است پشته TCP/IP و یا آداپتور شبکه مشکل داشته باشند.

شکل دستوری:

دستور ping به صورت **ping > IPمقصد <** می باشد. اگر پس از تایپ این دستوردر command) **cmd** (promot) وزدن کلید Enter پیغام Reply داده شد به مفهوم برقراری ارتباط با (command promot) وزدن کلید Enterپیغام کامپیوتری است که IP یا اسم آنرا جلوی این دستورزده ایم ودرصورت مشاهده ی پیغام های دیگری که در زیر مشاهده می کنید به صورت زیر عمل می کنیم:

The Destination Host Unreachable Message

این پیغام بدین معنی است که مسیری به کامپیوتر مقصد پیدا نشده است.برای حل این مشکل کامپیوترخود را وارسی کنید وببینید آیا تنظیمات آن به درستی انجام شده است یا خیر مطمئن شوید که **default gateway** درست تنظیم شده است.

شاید این پیغام را بسیاردیده باشید. این پیغام نشان دهنده این است که کامپیوتر شما درمدت مشخص تعیین شده ای پاسخ بسته ارسال شده را دریافت نکرده است. اگر فرض کنیم مسیر فیزیکی ارتباطی کامپیوترما با کامپیوترمقصد مشکلی نداشته باشد این پیغام می تواند نشانگر این مسئله باشد که کامپیوترمقصد به شبکه وصل نیست، خاموش بوده و یا به درستی تنظیم نشده است. همچنین این پیغام می تواند نشا نگراین باشد که یکی ازدستگاه های میانی درست کار نمی کند. دربرخی مواردخاص این پیغام به دلیل ترافیک بسیار بالای شبکه بوجودمی آید. همچنین ممکن است که عمل ping به آدرس شبکه اشتباهی صورت گرفته است یا اینکه آن کامپیوتردرشبکه صحیح وجود ندارد و باید اصلاح آدرس شبکه درآن صورت بگیرد.

در برخی موارد هم مشاهده می شود که پاسخ ping بصورت ممتد نمی باشد و گاه پاسخ به بسته اطلاعاتی ما قطع می شود. در این حالت معمولا نیاز است تا صحت دستگاه های میانی را بررسی کنید که آیا درست کار می کنند یا خیر. مشکل کارت شبکه هم به ندرت باعث این خطا می شود.

The Unknown Host Message

هرگاه آدرس مقصد قابلیت تشخیص توسط کامپیوترتان را نداشته باشد این پیغام را دریافت خواهید کرد. این پیغام معمولا وقتی ازآدرس مقصد اشتباه استفاده کنید اتفاق می افتد . همچنین عدم تنظیم DNS یا درست کار نکردن DNS هم امکان ایجاد این پیغام را می دهد.

درصورتی که موارد فوق راچک کردید وهنوز مشکل باقی باشد احتمال دارد مشکل **Name Resolution** باشید لذا باید **DNS**و **WINS**را بررسی کنید. شما می توانید از دستورات **nslookup**و **dig**برای این منظور استفاده کنید.

The Expired TTL Message

The Time To Liveیا **TTL**مطلبی جالب برای بررسی دستور Ping است.عمل TTL ازبه لوپ افتادن پاکت های پینگ جلوگیری می کند TTL . هاپ ها را در مسیر خود شمارش می کند و در هر هاپ یک شماره از TTL کم می شود. وقتی که عدد TTL به صفر برسد این بدان
معناست که زمان تعیین شده تمام شده و پیغام زیر نمایش داده می شود:

```
1                                    Reply from 24.67.180.1: TTL expired in transit
```

در صورتیکه این پیغام را دریافت کرده باشید به احتمال قوی مشکل **Routing**دارید. شما می توانید در TTL تغییر حاصل نمایید و برای این کار از دستور **ping –i**استفاده کنید.

رفع مشکل توسط دستور Ping

اگرچه دستور ping بطور کامل مشکل را حل نمی کند و احتمال خطا در نتیجه گیری با توجه به تجربه مدیرشبکه وجود خواهد داشت اما می توان تست های مفیدی رابرای تشخیص بهتر خطا با این دستور ساده انجام داد.

•آدرس لوپ بک کامپیوتر خود را توسط دستور **ping 127.0.0.1** بررسی کنید . درصورتیکه موفقیت ping شما ازسلامت TCP/IP دستگاه خود مطمئن خواهید شد در صورتیکه نتوانید آدرس لوپ بک راپینگ کنید به احتمال قوی باید TCP/IP دستگاه خود رادوباره نصب وتنظیم کنید.

•آدرس شبکه کارت شبکه خود را پینگ کنید درصورت موفقیت مطمئن خواهید شد که TCP/IP درست کار می کند ودرغیر اینصورت مشکل در تنظیم آدرس شبکه رو کارت شبکه دارید و یا ا ینکه کارت شبکه شما به درستی نصب نشده است.

•ادرس شبکه کامپیوتردیگرراپینگ کنید .بامشاهده پینگ موفق مطمئن خواهید شد که کامپیوتر شما درارتباط با کامپیوترهای دیگرروی شبکه ودیدن منابع مشکلی نخواهد داشت. درغیراین صورت ارتباط کامپیوتر شما به شبکه دارای مشکل است و باید اتصالات را بررسی کنید.

•پس از اطمینان از اینکه آدرس شبکه کامپیوتر شما درست کارمی کند وقادرهستید کامپیوتر های دیگردرشبکه را ببینید ، حال باید ببینید آیا کامپیوترشما کامپیوترهای خارج شبکه را نیز می تواند به راحتی ببیند یا خیر.برای این منظورباید آدرس Default Gateway را پینگ کنید.

•درصورتیکه که توانستید آدرس Default Gateway رادرمرحله قبل پینگ کنید حال می توانید اقدام به آدرس شبکه کامپیوتری خارج از شبکه خود را پینگ کنید.

•آدرس لوپ بک کامپیوتر خود را توسط دستور **ping 127.0.0.1**بررسی کنید. درصورتیکه موفقیت ping شما از سلامت TCP/IP دستگاه خود مطمئن خواهید شد. در صورتیکه نتوانید آدری لوپ بک را پینگ کنید به احتمال

قوی باید TCP/IP دستگاه خود را دوباره نصب و تنظیم کنید.

همانطورکه مشاهده کردید با انجام موارد بالابررسی خوبی برصحت ارتباط کامپیوتر خود خواهید داشت.درصورتیکه آدم خوشبینی هستید می تواند مرحله پنج را در ابتدا انجام دهید . ا گر پینگ درمحله پنج بدون مشکل انجام شود نشاندهنده آن است که کلیه مراحل بالا نیز
به خوبی کار می کنند و در غیر اینصورت از مرحله یک بررسی خود را شروع کنید.

سوئیچ ها:

دستور Ping معمولا بصورت تنها بکار برده می شود اما سوئیچ هایی نیز قابل استفاده با این دستور هستند . در زیر شرح برخی از این سوئیچ ها آمده است:

: Ping –t

میتوان تعیین کرد دستور Ping تا زمان interrupted شدن توسط کاربر به Ping کردن ادامه دهد. تا زمانی که عمل Ping کردن را بطوردستی قطع نکنیم عملیات ارسال ودریافت بسته اطلاعاتی ادامه پیدا خواهد کرد.برای توقف برنامه ping می توان از کلیدهایCTRL+C استفاده نمود.

: Ping –a

با این دستور میتوان نام IP **host** مورد نظر را پیدا کرد . به عبارتی این پارامتر نام host متناظر با ای پی را نمایش میدهد.(می توانیم به نام کامپیوتری که در حال Ping کردن هستیم دسترسی پیدا کنیم.

: Ping –n

میتوان تعداد دفعات ارسال **Echo Request messages**را که به طور پیش فرض ۴ بار میباشد افزایش یا کاهش داد.

طرز کار ping بدین صورت است که ابتدا بسته **ICMP Echo Request**را به سمت کامپیوترمقصد ارسال می کند اگرکامپیوتر مقابل این بسته را دریافت کند بسته ای به نامه **ICMP Echo Reply**رابه سمت مبداارسال می کند وخبر دریافت پاکت اطلاعاتی اولیه را بطور خودکار می دهد بطور پیش فرض تعداد ارسال بسته **Echo Request**چهارعدد است که در صورت استفاده از سوئیچ **t–**این تعداد بیشترخواهد گردید درصورتیکه روزخوبی داشته باشید وارتباط شما برقرارباشد پاسخ **Reply**رادریافت خواهید کرد و درغیر این صورت به پیغام **Time out**مواجهه خواهید شد وخب با این وضعیت باید دلیل عدم ارتباط را که ممکن است ناشی از مشکلات کارت شبکه و یا لینک فیزیکی شبکه باشد را بیابید.

: Ping –l

میتوان حجم بسته **Echo Request messages** را که به طورپیش فرض **32**بایت میباشد تغییرداد. ماکزیمم مقدار مجاز برای این پارامتر **65,527**میباشد.

Ping –I :

تنظیم TTL با همون **Time to live** یعنی مدت زمانی که packt برای دریافت جواب صبرمیکنه. میتوان مدت زمان زنده بودن packet سرگردان را تعیین کرد.

نکته:
مدتTTL برحسب مشخصات هاست تعیین میگردد به عنوان مثال اگرهاست مورد نظر Windows XP باشد مقدار TTL برابر **128** است.ماکزیمم این مقدار نیز **256** میباشد.

Ping –v :

میتوان مقدار **TOS – Type Of Service** در هدرای پی **Echo Request messages** را تعیین کرد . مقراد پیش فرض **0** میباشد.

Ping –w :

میتوان مدت زمان انتظار برای دریافت پاسخ از هاست بر حسب میلی ثانیه را تعیین نمود.

درصورتی که هاست دراین مدت زمان نتواند به بسته Echo Request messages دهد ازسرور **Request timed out** برای کاربرنمایش داده میشود.مقدار پیش فرض **4000**ms یا **4** ثانیه میباشد.

ping –r :

تعداد Hop را نمایش میده .یه عبارتی تعداد مسیری که Packet از اون عبور میکنه.

استفاده از Ping در ویندوز:

توضیحات:
- چهاربسته اطلاعاتی ارسال شده است که همان چهاربسته نیزدریافت شده اند (درزمان انتقال)
- هیچیک ازبسته های اطلاعاتی گم نشده اند
- زمان پاسخ حدودا" ۴۳۰ میلی ثانیه بوده است
- اندازه بسته های اطلاعاتی ارسالی ، سی و دو بایت است.

اشکال زدائی ارتباط بین گره های یک شبکه با استفاده از دستور Ping :

برای اشکال زدائی ارتباط بین گره های یک شبکه ، می توان مراحل زیر را دنبال نمود:

آیا پیکربندی TCP/IP بر روی سیسم محلی (ارسال کننده) درست است ؟

رای پاسخ به سوال فوق می توان آدرس IP سیستم محلی را Ping و نتایج را مشاهده نمود . در صورت عدم ارائه پاسخ مناسب ،می تواند مشکل مربوط به پیکربندی تنظیمات TCP/IP بر روی سیستم محلی باشد.

آیا امکان ping نمودن نام host وجود دارد ؟

برای پاسخ به سوال فوق به همراه دستور pingاز نام host استفاده نمائید ping قبل ازارسال بسته اطلاعاتی برای host مورد نظر، نام آن را به یک آدرس IP ترجمه می نماید اگر آدرسی که Ping ترجمه می نماید، آدرسی نیست که تصورآن را دارید می بایست پیکربندی سیستم خود را بررسی نمائید در چنین مواردی ممکن است شما کامپیوترخود را بگونه ای پیکربندی نموده اید که از یک آدرس IP خاص استفاده نماید ولی درسرویس دهنده **DNS**، به کامپیوتر شما یک آدرس IPدیگرمرتبط شده است در این رابطه می توان از دستور nslookup به منظور اشکال زدائی ترجمه استفاده نمود.

آیا امکان ارتباط با سیستمی دیگر در شبکه وجود دارد ؟

برای پاسخگوئی به سوال فوق می بایست یک سیستم دیگر را که مطمئن هستید در Subnet شما وجود دارد ، pingنمائید . در صورتی که نتایج موفقیت آمیز باشد ، شما می توانید با اعضاء **broadcast Domain** ارتباط برقرار نمائید.

آیا امکان ارتباط با Default Gateway وجود دارد ؟

Default Gatewayروتر ویا دستگاهی دیگراست که Subnet شما را به سایر شبکه ها متصل می نماید.درصورت عدم امکانping نمودن Default Gateway دواحتمال می تواند وجود داشته باشد:

احتمال اول : ممکن است آدرس **Subnet**شما اشتباه باشد . در چنین مواردی می بایست پیکربندی سیستم بررسی گردد تا این اطمینان حاصل شود که شما از یک آدرس درست برای روتر و یا host دیگر که مسئول فورواردینگ بسته های ا طلاعاتی در **Local Subnet**است ، استفاده می نمائید.

احتمال دوم : ممکن است خود Default gateway دارای مشکل باشد . برای اطمینان از این موضوع ، می توان از طریق یک سیستم دیگر موجود در شبکه ، Default Gatewayرا ping نمود . در صورتی که مشکل همچنان باقی است می بایست برای حل مشکل بر روی Default Gateway متمرکز گردید .

آیا امکان ارتباط با سایر سیستم های موجود در خارج از شبکه محلی وجود دارد ؟

برای پاسخ به سوال فوق ، می توان یک سیستم راه دور را ping نمود . در صورتی که عملیات توام با موفقیت باشد ، ارتباط شما از طریق Default gateway به درستی برقرارشده است و در صورت عدم موفقیت ، دلایل متعددی می تواند وجود داشته باشد: بروز اشکال در سیستم مقصد بروز اشکال در روتینگ به سیستم مقصد و یا تجهیزات موجود در خارج از شبکه محلی.

و اما دو نکته که بد نیست به آنان نیز اشاره ای داشته باشیم:

همانگونه که ملاحظه گردید ، دستور ping دارای امکاناتی مفید و قدرتمند به منظور اشکال زدائی ارتباط بین گره ها در شبکه های مبتنی بر TCP/IP است، ولی Ping of Death که احتمالا" نام آن را تاکنون شنیده اید دارای وضعیتی اینچنین نمی باشد Ping of Death یک نوع تهاجم در شبکه های کامپیوتری است که در آن یک مهاجم با استفاده از برنامه هائی خاص ، بسته های اطلاعاتی ICMP را تولید می نماید که دارای اندازه ای بیش از حد

مجازمی باشند . در صورتی که نرم افزارموجود بر روی سیستم مقصد به درستی **Patch**نشده باشد بسته های اطلاعاتی ارسالی توسط مهاجمان دریافت و بخش عمده ای ازحافظه رااشغال نموده ومی تواند سرریزحافظه رابدنبال داشته باشد مدیران شبکه می بایست یک محیط ایمن به منظوراستفاده از pingرا در شبکه فراهم نموده تا امکان تحقق چنین حملاتی در شبکه وجود نداشته باشد.

نکته دوم:

در صورتی که نتوان یک کامپیوترراه دور را ping نمود ، نمی توان با قاطعیت اعلام نمود که سیستم مقصد به شبکه متصل نمی باشد و یا مشکل مربوط به کابل کشی شبکه است . در این رابطه دلایل متعددی می تواند وجود داشته باشد:

بروزاشکال درهریک ازدستگاه های موجود درمسیرارتباطی نظیر هاب ، سوئیچ ،روترو یا Default Gateway به همین دلیل ، می بایست همواره یک طرح کامل از شبکه به همراه جزئیات مربوطه وجود داشته باشد تا درصورت بروز مشکلاتی اینچنین به سرعت بتوان
مسیر مربوطه را برای اشکال زدائی بررسی نمود در چنین مواردی، می بایست هر دستگاه موجود در مسیر ارتباطی بررسی گردد.