Author:Satanic Soulful

Network

TCP/IP

Introduction to Transmission Control Protocol/Internet Protocol

SatanicHell-Shabgard

Satanic Hell

جهنم شیطانی

TCP/IP

مباحثی پیرامون تی سی پی / آی پی

نویسنده: Satanic Soulful
تاریخ:19/03/1384

Contact:
Satanic.soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Special TNX♥2:
Hell Hacker – **C0llecT0r –** S hahro Z – XshabgardX –Rap Game-Dr.Hoshmand & Dr.Sohyli

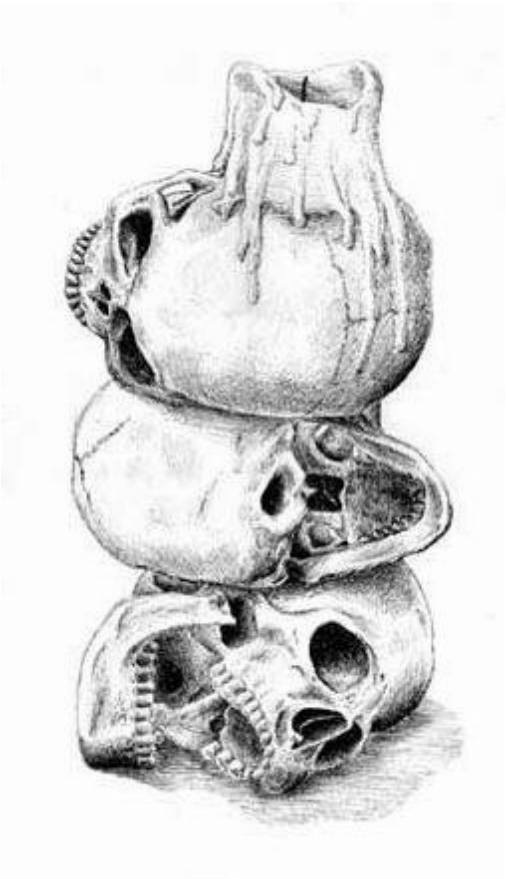
ملاحضات:

لازم به تذکر است کلیه مطالب گفته شده تنها جنبه آموزشی دارد و
هر گونه استفاده غیر آموزشی به عهده خود کاربر می باشد و نویسنده این مقاله و مدیریت سایت شبگرد و جهنم شیطانی هیچ گونه مسولیتی نسبت به استفاده نادرست از این مقاله را برعهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروهای مربوط بلامانع است.

منابع:

"Ip Routing" by Ravi Malhotra ,"DNS & BIND CookBook" by Cricket Liu
"Internet Core Protocols"by Eric A. Hall ,"Ethernet"by Charles , SCRCO
"TCP/IP Network Administration" by Craig Hunt , 'High Performance TCP/IP Networking' & جزوات و نوشته های دکتر هوشمند و دکتر سهیلی



به خاطر سه کس : غریب , تنها , بیکس

مقدمه:
در این مقاله مباحثی اندک راجبه یکی از پروتکل های مهم اینترنت را به شما میگویم, البته این توضیحات فقط برای درک بهتر شما از این پروتکل است و به صورت خلاصه است و فقط نکته و بعضی از تعریف ها است.

TCP/IP ، یکی از مهمترین پروتکل های استفاده شده در شبکه های کامپیوتری است اینترنت بعنوان بزرگترین شبکه موجود ، از پروتکل فوق بمنظور ارتباط دستگاه های متفاوت استفاده می نماید. پروتکل ، مجموعه قوانین لازم بمنظور قانونمند نمودن نحوه ارتباطات در شبکه های کامپیوتری است .
امروزه اکثر شبکه های کامپیوتری بزرگ و اغلب سیستم های عامل موجود از پروتکل TCP/IP ، استفاده و حمایت می نمایند. TCP/IP ، امکانات لازم بمنظور ارتباط سیستم های غیرمشابه را فراهم می آورد. از ویژگی های مهم پروتکل فوق ، می توان به مواردی همچون : قابلیت اجراء بر روی محیط های متفاوت ، ضریب اطمینان بالا ،قابلیت گسترش و توسعه آن ، اشاره کرد .
از پروتکل فوق، بمنظور دستیابی به اینترنت و استفاده از سرویس های متنوع آن نظیر وب و یا پست الکترونیکی استفاده می گردد.
تنوع پروتکل های موجود در پشته TCP/IP و ارتباط منطقی و سیستماتیک آنها با یکدیگر، امکان تحقق ارتباط در شبکه های کامپیوتری را با اهداف متفاوت ، فراهم می نماید.
فرآیند برقراری یک ارتباط ، شامل فعالیت های متعددی نظیر : تبدیل نام کامپیوتر به آدرس IP معادل ، مشخص نمودن موقعیت کامپیوتر مقصد ، بسته بندی اطلاعات ، آدرس دهی و روتینگ داده ها بمنظور ارسال موفقیت آمیز به مقصد مورد نظر ، بوده که توسط مجموعه پروتکل های موجود در پشته TCP/IP انجام می گیرد.
TCP/IP پروتکل استاندارد در اکثر شبکه های بزرگ است . با اینکه پروتکل فوق کند و مستلزم استفاده از منابع زیادی است ، ولی بدلیل مزایای بالای آن نظیر : قابلیت روتینگ ، حمایت در اغلب پلات فورم ها و سیستم های عامل همچنان در زمینه استفاده از پروتکل ها حرف اول را می زند.
با استفاده از پروتکل فوق کاربران با در اختیار داشتن ویندوز و پس از اتصال به شبکه اینترنت، براحتی قادر به ارتباط با کاربران دیگر خواهند بود که از مکینتاش استفاده می کند.
امروزه کمتر محیطی را می توان یافت که نیازبه دانش کافی در رابطه با TCP/IP نباشد. حتی سیستم عامل شبکه ای ناول که سالیان متمادی از پروتکل IPX/SPX برای ارتباطات استفاده می کرد، در نسخه شماره پنج خود به ضرورت استفاده از

پروتکل فوق واقف و نسخه اختصاصی خود را در این زمینه ارائه نمود.
پروتکل TCP/IP در ابتدا برای استفاده در شبکه ARPAnet (نسخه قبلی اینترنت) طراحی گردید.
وزارت دفاع امریکا با همکاری برخی از دانشگاهها اقدام به طراحی یک سیستم جهانی نمود که دارای قابلیت ها و ظرفیت های متعدد حتی در صورت بروز جنگ هسته ای باشد. پروتکل ارتباطی برای شبکه فوق ، TCP/IP در نظر گرفته شد.

TCP/IPچیست؟

کلید اجرای یک سرویس کوچک برنامه نویسی TCP/IP می باشد .
Internet Protocol / Transmission Control Protocolعنوانی است برای گروهی از پروتکل ها که در جهت برفراری ارتباط کامپیوتر ها استفاده می شود .
سرویس دهنده ماشینی است که اطلاعات را بر روی سرویس گیرنده ارسال می کند .
سرویس گیرنده یک کاربر عمومی اینترنت و یا اینترانت می باشد و کد ورود به شبکه با استفاده از یک نرم افزار صورت می گیرد .

چهار لایه : TCP/IP

لایه واسطه شبکه
لایه شبکه
لایه انتقال
لایه کاربرد

لایه اول : لایه واسطه شبکه
در این لایه استانداردهای سخت افزاری و نرم افزاری و پرتکل های شبکه تعریف شده .
این لایه درگیر با مسائل سخت افزاری مرتبط با شبکه بوده و می تواند عناصر همگن و ناهمگن را به هم پیوند بزند. در این لایه تمام پروتکل های LAN ,MAN قابل استفاده هستند .

لایه دوم : لایه شبکه
وظیفه اصلی این لایه هدایت از مبدا تا مقصد بسته های اطلاعاتی خاص به نام IP است .
به غیر از پروتکل IP پروتکل هایی دیگ نیز هستند که وظایف مهمی را بر عهده دارند .

مهمترین آنها ARP , RARP , RIP , ICMP , BOOTP ,& more :
در این لایه مسیر یاب ها از شرایط توپولوژیکی و ترافیکی شبکه اطلاعات را کسب می کند تا مسیر یاب ها به روش آسان و پویا انجام دهند .

لایه سوم : لایه انتقال
در این لایه ماشین ها ی میزبان در شبکه با هم ارتباط برقرار می کنند و به عبارت دیگر یک سرویس اتصال گرا مطمئن است برای عملیاتی مانند ارسال صوت و تصویر که سرعت مهمتر از دقت است سرویس های سریع و نا مطمئن طراحی شده است. در این سرویس لایه از رسیدن داده ها به مقصد اطلاع می یابد .

لایه چهارم : لایه کاربرد
این لایه دارای سطع بالایی برای خلق برنامه های کاربردی ویژه و پیچیده ارائه می شود .
انتقال فایل یا FTP و شبیه سازی ترمینال و مدیریت پست و انتقال صفحات ابر متنی و ده ها پروتکل کاربردی دیگر از سطح این لایه است.

اجزای پروتکل TCP/IP
پروتکل TCP/IP از مجموعه پروتکل های دیگر تشکیل شده که هر یک در لایه مربوطه، وظایف خود را انجام می دهند. پروتکل های موجود در لایه های Transport و Network دارای اهمیت بسزائی بوده و در ادامه به بررسی آنها خواهیم پرداخت .

پروتکل های موجود در لایه Network پروتکل TCP/IP

1- پروتکل (**TCP**) Protocol Transmission Control ، مهمترین وظیفه پروتکل فوق اطمینان از صحت ارسال اطلاعات است . پروتکل فوق اصطلاحا" Connection-oriented نامیده می شود.

علت این امر ایجاد یک ارتباط مجازی بین کامپیوترهای فرستنده و گیرنده بعد از ارسال اطلاعات است . پروتکل هائی از این نوع ، امکانات بیشتری را بمنظور کنترل خطاهای احتمالی در ارسال اطلاعات فراهم نموده ولی بدلیل افزایش بار عملیاتی سیستم کارائی آنان کاهش خواهد یافت .

از پروتکل TCP بعنوان یک پروتکل قابل اطمینان نیز یاد می شود. علت این امر ارسال اطلاعات و کسب آگاهی لازم از گیرنده اطلاعات بمنظور اطمینان از صحت

ارسال توسط فرستنده است . در صورتیکه بسته های اطلاعاتی بدرستی دراختیار فرستنده قرار نگیرند، فرستنده مجددا" اقدام به ارسال اطلاعات می نماید.

2- پروتکل (**UDP**)User Datagram Protocol . پروتکل فوق نظیر پروتکل TCP در لایه " حمل " فعالیت می نماید. UDP بر خلاف پروتکل TCP بصورت " بدون اتصال " است . بدیهی است که سرعت پروتکل فوق نسبت به TCP سریعتر بوده ولی از بعد کنترل خطاء تظمینات لازم را ارائه نخواهد داد. بهترین جایگاه استفاده از پروتکل فوق در مواردی است که برای ارسال و دریافت اطلاعات به یک سطح بالا از اطمینان ، نیاز نداشته باشیم .

3- پروتکل(**IP**)Internet Protocol . پروتکل فوق در لایه شبکه ایفای وظیفه کرده و مهمترین مسئولیت آن دریافت و ارسال بسته های اطلاعاتی به مقاصد درست است . پروتکل فوق با استفاده از آدرس های نسبت داده شده منطقی، عملیات روتینگ را انجام خواهد داد.

پروتکل ها در لایه Application پروتکل TCP/IP

پروتکل TCP/IP صرفا" به سه پروتکل TCP، UDP و IP محدود نشده و در سطح لایه Application دارای مجموعه گسترده ای از سایر پروتکل ها است . پروتکل های فوق بعنوان مجموعه ابزارهائی برای مشاهده ، اشکال زدائی و اخذ اطلاعات و سایر عملیات مورد استفاده قرار می گیرند.در این بخش به معرفی برخی از این پروتکل ها خواهیم پرداخت .

1- پروتکل (**FTP**)File Transfer Protocol . از پروتکل فوق برای تکثیر فایل های موجود بر روی یک کامپیوتر و کامپیوتر دیگر استفاده می گردد. ویندوز دارای یک برنامه خط دستوری بوده که بعنوان سرویس گیرنده ایفای وظیفه کرده و امکان ارسال و یا دریافت فایل ها را از یک سرویس دهنده FTP فراهم می کند.

2- پروتکل(**SNMP**)Simple Network Management Protocol . از پروتکل فوق بمنظور اخذ اطلاعات آماری استفاده می گردد. یک سیستم مدیریتی، درخواست خود را از یک آژانس SNMP مطرح و ماحصل عملیات کار در یک (MIB)Management Information Base ذخیره می گردد. MIB یک بانک اطلاعاتی بوده که اطلاعات مربوط به کامپیوترهای موجود در شبکه را در خود نگهداری می نماید .(مثلا" چه میزان فضا ی هارد دیسک وجود دارد)

3- پروتکل **TelNet** . با استفاده از پروتکل فوق کاربران قادر به log on ، اجرای برنامه ها و مشاهده فایل های موجود بر روی یک کامپیوتر از راه دور می باشند. ویندوز دارای برنامه های سرویس دهنده و گیرنده جهت فعال نمودن و استفاده از پتانسیل فوق است .

4- پروتکل (**SMTP**)simple Mail Transfer Protocol . از پروتکل فوق برای ارسال پیام الکترونیکی استفاده می گردد.

5- پروتکل(**HTTP**)HyperText Transfer Protocol . پروتکل فوق مشهورترین پروتکل در این گروه بوده و از آن برای رایج ترین سرویس اینترنت یعنی وب استفاده می گردد. با استفاده از پروتکل فوق کامپیوترها قادر به مبادله فایل ها با فرمت های متفاوت (متن، تصاویر ،گرافیکی ، صدا، ویدئو و...) خواهند بود. برای مبادله اطلاعات با استناد به پروتکل فوق می بایست ، سرویس فوق از طریق نصب سرویس دهنده وب فعال و در ادامه کاربران و استفاده کنندگان با استفاده از یک مرورگر وب قادر به استفاده از سرویس فوق خواهند بود.

6-پروتکل(**NNTP**)Network News Transfer Protocol . از پروتکل فوق برای مدیریت پیام های ارسالی برای گروه های خبری خصوصی و عمومی استفاده می گردد. برای عملیاتی نمودن سرویس فوق می بایست سرویس دهنده NNTP بمنظور مدیریت محل ذخیره سازی پیام های ارسالی نصب و در ادامه کاربران و سرویس گیرندگان با استفاده از برنامه ای موسوم به NewsReader از اطلاعات ذخیره شده استفاده خواهند کرد

IGMP Internet Group Managemant Protocol . پروتکل فوق ، مسئول مدیریت Multicasting در TCP/IP را برعهده دارد.

لایه Network Interface

لایه " اینترفیس شبکه " ، مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده از محیط انتقال شبکه است . لایه فوق ، شامل دستگاه های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است . کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده (نظیر : B5-50-04-22-D4-66) بوده که آدرس MAC ، نامیده می شود. لایه " اینترفیس شبکه " ، شامل پروتکل های مبتنی بر نرم افزار مشابه لایه های قبل ، نمی باشد. پروتکل های Ethernet و Asynchronous Transfer Mode(ATM) ، نمونه هائی از پروتکل های موجود در این لایه می باشند .

پروتکل های فوق ، نحوه ارسال داده در شبکه را مشخص می نمایند.
مشخص نمودن برنامه ها در شبکه های کامپیوتری ، برنامه ها ی متعددی در یک زمان با یکدیگر مرتبط می گردند.

زمانیکه چندین برنامه بر روی یک کامپیوتر فعال می گردند ، TCP/IP ، می بایست از روشی بمنظور تمایز یک برنامه از برنامه دیگر، استفاده نماید. بدین منظور ، از یک سوکت (Socket) بمنظور مشخص نمودن یک برنامه خاص ، استفاده می گردد.
آدرس IP :برقراری ارتباط در یک شبکه ، مستلزم مشخص شدن آدرس کامپیوترهای مبداء و مقصد است (شرط اولیه بمنظور برقراری ارتباط بین دو نقطه ، مشخص بودن آدرس نقاط درگیر در ارتباط است) . آدرس هر یک از دستگاه های درگیر در فرآیند ارتباط ، توسط یک عدد منحصربفرد که IP نامیده می شود ، مشخص می گردند. آدرس فوق به هریک از کامپیوترهای موجود در شبکه نسبت داده می شود . IP : 10. 10.1.1 ، نمونه ای در این زمینه است.

مدل آدرس دهی IP

علاوه بر جایگاه پروتکل ها، یکی دیگر از عناصر مهم در زیرساخت شبکه های مبتنی بر TCP/IP مدل آدرس دهی IP است . مدل انتخابی می بایست این اطمینان را بوجود آورد که اطلاعات ارسالی بدرستی به مقصد خواهند رسید. نسخه شماره چهار IP (نسخه فعلی) از 32 بیت برای آدرس دهی استفاده کرده که بمنظور تسهیل در امر نمایش بصورت چهار عدد صحیح (مبنای ده) که بین آنها نقطه استفاده شده است نمایش داده می شوند.

نحوه اختصاص IP

نحوه اختصاص IP به عناصر مورد نیاز در شبکه های مبتنی بر TCP/IP یکی از موارد بسیار مهم است . اختصاص IP ممکن است بصورت دستی و توسط مدیریت شبکه انجام شده و یا انجام رسالت فوق بر عهده عناصر سرویس دهنده نرم افزاری نظیر DHCP و یا NAT گذاشته گردد

عملیات انجام شده توسط IP

می توان IP را بعنوان مکانی در نظر گرفت که عملیات مرتب سازی و توزیع بسته های اطلاعاتی در آن محل ، صورت می پذیرد .بسته ها ی اطلاعاتی توسط یکی از پروتکل های لایه حمل (TCP و یا UDP) و یا از طریق لایه " اینترفیس شبکه " ، برای IP ارسال می گردند . اولین وظیفه IP ، روتینگ بسته های اطلاعاتی بمنظور ارسال به مقصد نهائی است . هر بسته اطلاعاتی ، شامل آدرس IP مبداء (فرستنده) و آدرس IP مقصد (گیرنده) می باشد. در صورتیکه IP ، آدرس مقصدی را

مشخص نماید که در همان سگمنت موجود باشد ، بسته اطلاعاتی مستقیما" برای کامپیوتر مورد نظر ارسال می گردد . در صورتیکه آدرس مقصد در همان سگمنت نباشد ، IP ، می بایست از یک روتر استفاده و اطلاعات را برای آن ارسال نماید.یکی دیگر از وظایف IP ، ایجاد اطمینان از عدم وجود یک بسته اطلاعاتی (بلاتکلیف !) در شبکه است . بدین منظور محدودیت زمانی خاصی در رابطه با مدت زمان حرکت بسته اطلاعاتی در طول شبکه ، در نظر گرفته می شود .عملیات فوق، توسط نسبت دادن یک مقدار Time To Live(TTL) به هر یک از بسته های اطلاعاتی صورت می پذیرد. TTL ، حداکثر مدت زمانی را که بسته اطلاعاتی قادر به حرکت در طول شبکه است را مشخص می نماید(قبل از اینکه بسته اطلاعاتی کنار گذاشته شود) .

Subnetting

یکی از مهمترین عملیات در رابطه با اختصاص IP مسئله Subnetting است . مسئله فوق بعنوان هنر و علمی است که ماحصل آن تقسیم یک شبکه به مجموعه ای از شبکه های کوچکتر (Subnet) از طریق بخدمت گرفتن ۳۲ بیت با نام Subnet mask بوده که بنوعی مشخصه (ID) شبکه را مشخص خواهد کرد.

کالبد شکافی آدرس های IP

هر دستگاه در شبکه های مبتنی بر TCP/IP دارای یک آدرس منحصر بفرد است . آدرس فوق IP نامیده می شود. یک آدرس IP مطابق زیر است :

- 216.27.61.137

بمنظور بخاطر سپردن آسان آدرس های IP ، نحوه نما یش آنها بصورت دسیمال (مبنای دهدهی) بوده که توسط چهار عدد که توسط نقطه از یکدیگر جدا می گردند ، است . هر یک از اعداد فوق را octet می گویند. کامپیوترها برای ارتباط با یکدیگر از مبنای دو (باینری) استفاده می نمایند. فرمت باینری آدرس IP اشاره شده بصورت زیر است :

- 11011000.00011011.00111101.10001001

همانگونه که مشاهده می گردد ، هر IP از 32 بیت تشکیل می گردد. بدین ترتیب می توان حداکثر 4.294.967.296 آدرس منحصر بفرد را استفاده کرد(2^{32}) .

مثلا" آدرس 255.255.255.255 برای Broadcast (انتشار عام) استفاده می گردد . نمایش یک IP بصورت چهار عدد (Octet) صرفا" برای راحتی کار نبوده و از آنان برای ایجاد " کلاس های IP " نیز استفاده می گردد. هر Octet به دو بخش مجزا تقسیم می گردد: **شبکه** (Net) و **میزبان** (Host) . اولین octet نشاندهنده شبکه بوده و از آن برای مشخص نمودن شبکه ای که کامپیوتر به آن تعلق دارد ، استفاده می گردد. سه بخش دیگر octet ، نشاندهنده آدرس کامپیوتر موجود در شبکه است

پنج کلاس متفاوت IP بهمراه برخی آدرس های خاص ، تعریف شده است :

- **Default Network** . آدرس IP **0.0.0.0** ، برای شبکه پیش فرض در نظر گرفته شده است .آدرس فوق برای مواردیکه کامپیوتر میزبان از آدرس خود آگاهی ندارد استفاده شده تا به پروتکل هائی نظیر DHCP اعلام نماید برای وی آدرسی را تخصیص دهد.

- **کلاس A** . کلاس فوق برای شبکه های بسیار بزرگ نظیر یک شرکت بین المللی در نظر گرفته می شود. آدرس هائی که اولین octet آنها 1 تا 126 باشد ، کلاس A می باشند. از سه octet دیگر بمنظور مشخص نمودن هر یک از کامپیوترهای میزبان استفاده می گردد. بدین ترتیب مجموع شبکه های کلاس A ، معادل 126 و هر یک از شبکه های فوق می توانند 16.777.214 کامپیوتر میزبان داشته باشند. (عدد فوق از طریق حاصل $2^{24} - 2$ بدست آمده است) .بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس A معادل 2.147.483.648 (2^{31}) است . در شبکه های کلاس A ، بیت با ارزش بالا در اولین octet همواره مقدار صفر را دارد.

Host (Node)	NET
24.53.107	**115.**

- **LoopBack** . آدرس IP 127.0.0.1 برای LoopBack در نظر گرفته شده است . کامپیوتر میزبان از آدرس فوق برای ارسال یک پیام برای خود استفاده می کند.(فرستنده و گیرنده پیام یک کامپیوتر می باشد) آدرس فوق اغلب برای تست و اشکال زدائی استفاده می گردد.

- **کلاس B** . کلاس فوق برای شبکه های متوسط در نظر گرفته می شود.(مثلا" یک دانشگاه بزرگ) آدرس هائی که اولین octet آنها 128 تا 191 باشد ، کلاس B می باشند. در کلاس فوق از دومین octet هم برای مشخص کردن شبکه استفاده می گردد. از دو octet دیگر برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد بدین ترتیب 16.384 (2^{14}) شبکه از نوع کلاس B وجود دارد. تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل 65.534 (2 - 2^{16}) است . بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس B معادل 1.073.741.824 (2^{30}) است در شبکه های کلاس B ، اولین و دومین بیت در اولین octet به ترتیب مقدار یک و صفر را دارا می باشند.

Host (Node)	NET
53.107	**145.24.**

- **کلاس C** . کلاس فوق برای شبکه های کوچک تا متوسط در نظر گرفته می شود.آدرس هائی که اولین octet آنها 192 تا 223 باشد ، کلاس C می باشند. در کلاس فوق از دومین و سومین octet هم برای مشخص کردن شبکه استفاده می گردد. از آخرین octet برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد . بدین ترتیب 2.097.152 (2^{21}) شبکه کلاس C وجود دارد.تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل 254 (2 - 2^{8}) است . بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس C معادل 536.870.912 (2^{29}) است . در شبکه های کلاس C ، اولین ، دومین و سومین بیت در اولین octet به ترتیب مقدار یک ، یک و صفر را دارا می باشند.

Host(Node)	NET
107	**195.24.53.**

- **کلاس D** . از کلاس فوق برای multicasts استفاده می شود. در چنین حالتی یک گره (میزبان) بسته اطلاعاتی خود را برای یک گروه خاص ارسال می دارد. تمام دستگاه های موجود در گروه ، بسته اطلاعاتی ارسال شده را دریافت خواهند کرد. (مثلا" یک روتر سیسکو آخرین وضعیت بهنگام شده خود را برای سایر روترهای سیسکو ارسال می دارد) کلاس فوق نسبت به سه کلاس قبلی دارای ساختاری کاملا" متفاوت است. اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و صفر می باشند.28 بیت باقیمانده بمنظور مشخص نمودن گروههائی از

کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی 268.435.456 (2^{26}) کامپیوتر است

Host(Node)	NET
24.53.107	224.

- **کلاس E** . از کلاس فوق برای موارد تجربی استفاده می شود. کلاس فوق نسبت به سه کلاس اولیه دارای ساختاری متفاوت است . اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و یک می باشند.28 بیت باقیمانده بمنظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی 268.435.456 (2^{26}) کامپیوتر است

Host(Node)	NET
24.53.107	240.

- **BroadCast** . پیام هائی با آدرسی از این نوع ، برای تمامی کامپیوترهای در شبکه ارسال خواهد شد. این نوع پیام ها همواره دارای آدرس زیر خواهند بود :

- **255.255.255.255**.

- **آدرس های رزو شده** . آدرس های IP زیر بمنظور استفاده در شبکه های خصوصی (اینترانت) رزو شده اند :

- 10.x.x.x
- 172.16.x.x - 172.31.x.x
- 192.168.x.x

- **IP نسخه شش** . نسخه فوق برخلاف نسخه فعلی که از 32 بیت بمنظور آدرس دهی استفاده می نماید ، از 128 بیت برای آدرس دهی استفاده می کند. هر شانزده بیت بصورت مبنای شانزده نمایش داده می شود. :

2b63:1478:1ac5:37ef:4e8c:75df:14cd:93f2

خلاصه :

4th Octet	3rd Octet	2nd Octet	1st Octet	Class
Host ID			Net ID	A
Host ID		Net ID		B
Host ID		Net ID		C

Comments	Normal Netmask	Address Range	Network Type
For very large networks	255.0.0.0	001.x.x.x to 126.x.x.x	Class A
For medium size networks	255.255.0.0	128.1.x.x to 191.254.x.x	Class B
For small networks	255.255.255.0	192.0.1.x to 223.255.254.x	Class C
Used to support multicasting		224.x.x.x to 239.255.255.255	Class D
		240.x.x.x to 247.255.255.255	Class E

فیلترینگ بسته های اطلاعاتی

TCP/IP یکی از پروتکل های کاملا" شناخته شده در عرصه شبکه های کامپیوتری است که در عمل تا اندازه ای پیچیده جلوه می نماید . شاید بخشی از این پیچیدگی مبتنی بر این حقیقت باشد که پروتکل فوق از تعداد زیادی زیرعنصر نظیر پورت ها و پروتکل های دیگر تشکیل شده است . پروتکل TCP/IP به منظور انجام عملیات روزمره خود به تعداد زیادی از پورت ها و پروتکل ها نیاز خواهد داشت و برخی دیگر بندرت استفاده می گردند . پروتکل های غیرضروری می تواند امنیت شبکه شما را بمخاطره انداخته و فرصت نفوذ به یک شبکه را در اختیار مهاجمان قرار دهد .
برای پیشگیری از دستیابی غیر مجاز مهاجمان به شبکه ، اغلب مدیران شبکه اقدام به پیاده سازی یک فایروال می نمایند که در آن تمامی پورت ها و پروتکل های غیرضروری ، بلاک می گردند.
شاید این موضوع برای شما جالب باشد که بدانید نسخه های ویندوز 2000 به بعد دارای امکانات از قبل تعبیه شده ای نظیر پتانسیل های ارائه شده توسط فایروال ها می باشند . در ادامه با نحوه بلاک کردن پورت ها و پروتکل های غیرضروری در نسخه ویندوز 2000 آشنا می شویم .
اجازه دهید در ابتدا با صراحت عنوان نمائیم که راه حلی که در ادامه به آن اشاره خواهد شد را نمی توان به عنوان گزینه ای جایگزین در مقابل یک فایروال واقعی مطرح نمود . فیلترینگ بسته های اطلاعاتی TCP/IP با استفاده از امکانات ارائه شده در نسخه های ویندوز 2000 به بعد ، صرفا" روشی است که می تواند تا حدودی شبکه شما را ایمن نماید .
سیستم فیلترینگ بسته های اطلاعاتی در ویندوز 2000 بگونه ای طراحی شده است که تمامی بسته های اطلاعاتی فیلتر می گردند مگر آنانی که مجوز لازم برای استفاده از آنان صادر و اصطلاحا" در لیست مجاز قرار گرفته باشند . پیشنهاد می گردد تمامی بسته های اطلاعاتی بجزء آنانی که به مقصد شماره پورت های زیر حرکت می نمایند ، بلاک گردند .

- شماره پورت های TCP

شماره پورت های TCP	
شماره پورت	کاربرد
20	FTP Server Data Channel
21	FTP Server Control Channel

23	Telnet
80	HTTP
139	NetBIOS

- شماره پورت های UDP

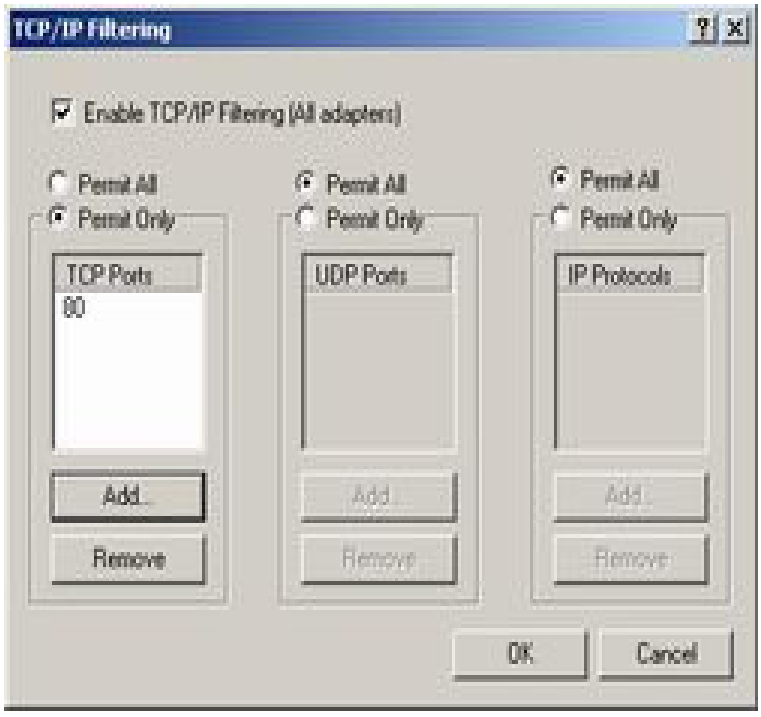
شماره پورت های UDP	
شماره پورت	کاربرد
53	DNS Lookup
69	TFTP
137	NBNS
161	SNMP
520	RIP

- شماره پورت های IP

شماره پورت های UDP	
شماره پورت	کاربرد
1	ICMP
2	IGMP
3	GGP
4	IP in IP encapsulation
5	ST stream
6	TCP
7	Often used for Computer Based Training
8	EGP

نحوه فلیترینگ پورت ها و پروتکل های غیرضروری

- کلیک بر روی آیکون Dial Up Connections Network and از طریق control panel
- کلیک سمت راست بر روی Connection مورد نظری که قصد پیکربندی آن را داریم و انتخاب گزینه Properties
- انتخاب پروتکل TCP/IP از طریق لیست عناصر نصب شده و فعال نمودن دکمه Properties
- کلیک بر روی دکمه Advanced (پس از نمایش صفحه مربوط به خصلت ها ی پروتکل TCP/IP)
- انتخاب گزینه TCP/IP Filtering و کلیک بر روی دکمه Properties . در ادامه پنجره Filtering TCP/IP نمایش داده می شود :



همانگونه که در شکل فوق مشاهده می گردد ، در قسمت بالای پنجره TCP/IP Filtering یک check box به منظور فعال و یا غیرفعال نمودن (Enable All Adapters) TCP/IP Filtering وجود دارد . پنجره فوق به سه ستون TCP Ports , UDP Ports و IP Protocols تقسیم شده است که هر یک دارای مجموعه ای از دکمه های Radio button می باشند . مقدار پیش فرض Radio button موجود در هر ستون، Permit All در نظر گرفته شده است . بدین ترتیب به تمامی بسته های اطلاعاتی این اجازه داده می شود که بدون هیچگونه فیلترینگی در

مسیر خود آزادانه حرکت نمایند .
برای اعمال فیلترینگ بر روی برخی پورت ها می توان مقدار Radio button موجود در هر ستون را به Only Permit تغییر داد . بدین ترتیب صرفا" به شماره پورت های مشخص شده در لیست ، اجازه ارسال و یا دریافت بسته های اطلاعاتی از طریق connection مربوطه داده می شود . . با استفاده از دکمه های Add و یا Remove می توان لیست پورت های مجاز را ویرایش نمود . مثلا" در صورتی که بخواهیم به connection مورد نظر امکان دستیابی به صفحات وب داده شود ، می توان پورت 80 را در بخش TCP Ports اضافه نمود .
فیلترینگ بسته های اطلاعاتی با بلاک نمودن بسته های اطلاعاتی غیرمجاز می تواند یک سطح حفاظتی را به شبکه شما اضافه می نماید. در صورتی که پس از ایجاد لیست پورت های ضروری (بر اساس جداول اشاره شده) با مشکل خاصی برخورد کردید ، ممکن است برنامه ها و یا سرویس هائی در شبکه شما استفاده می گردد که از پورت های خاص دیگری استفاده می نمایند . در صورت تحقق چنین شرایطی می توان یا شماره پورت حذف شده را به لیست مورد نظر اضافه نمود و یا Packet filtering را غیرفعال تا همه چیز به حالت اولیه بر گردد .

بررسی وضعیت پیکربندی TCP/IP

پیکربندی TCP/IP ، معمولا" در زمان نصب سیستم عامل انجام می شود . در برخی موارد ممکن است لازم باشد که تنظیمات انجام شده ، تغییر یابند. مثلا" در صورتی که کامپیوتر به یک subnet دیگر منتقل شده است ، می بایست تغییرات ضروری را بر روی آن اعمال نمود (آیا سیستم دارای یک آدرس IP است که دارای شماره شبکه ای یکسان و مشابه سایر کامپیوترهای موجود در شبکه است ؟) . اطمینان از صحت تنظیمات Mask Subnet و Default gateway از دیگر اقدامات ضروری در این رابطه است . در صورتی که از DHCP به منظور نسبت دهی اطلاعات پیکربندی TCP/IP (نظیر آدرس IP) استفاده می شود ، می بایست از وجود یک سرویس دهنده DHCP و یا یک DHCP relay agent در subnet جدید ، اطمینان حاصل نمود .
در صورتی که همه تنظیمات به درستی انجام شده است ولی همچنان سیستم دارای مشکل است ، می توان از ابزارهائی که به همراه اکثر نسخه های TCP/IP ارائه شده است ، استفاده نمود .

استفاده از hostname

یکی از عملیات اولیه به منظور اشکال زدائی یک کامپیوتر موجود درشبکه ، تشخیص نام آن است. بدین منظور می توان از برنامه کاربردی hostname استفاده نمود . برای نامگذاری کامپیوترها از دو روش متفاوت استفاده می شود .

در اولین روش ، اسامی flat (غیرسلسله مراتبی) با استفاده از جداولی نظیر host tables به دستگاه ها نسبت داده می شوند . در روش دوم ، از طریق سرویس دهنده DNS یک نام به دستگاه موجود در شبکه ، نسبت داده می شود (از دستور hostname در دو روش فوق می توان استفاده نمود) .
hostname ، ساده ترین دستوری است که می توان با استفاده از آن بررسی اولیه پیکربندی یک کامپیوتر را انجام داد . در سیستم های مبتنی بر ویندوز ، دستور فوق نام کامپیوتر را نمایش خواهد داد . برای استفاده از دستور فوق ، کافی است نام آن را از طریق پنجره command prompt تایپ نمود .

دستور تایپ	خروجی
C:\>hostname	Satanichell

ضرورت استفاده از دستور hostname

شاید این سوال برای شما مطرح شده باشد که چرا می بایست از دستور hostname استفاده نمائیم و نتایجی که نمایش داده می شود ، بیانگر چه واقعیتی است ؟ با توجه به این که hostname به یک آدرس IP ترجمه شده است ، با استفاده از دستور فوق ، می توان از صحت آدرس IP مرتبط با نام ، اطمینان حاصل نمود .
از دستور hostname بر روی سیستم هائی که بر روی آنان سیستم عامل یونیکس و یا لینوکس نصب شده است نیز استفاده می گردد . با توجه به نوع سیستم عامل ، نحوه پیکربندی و پارامترهای استفاده شده ، اجرای این دستور نتایج متفاوتی را بدنبال خواهد داشت. در سیستم های عامل ویندوز NT/2000/XP ، دستور فوق نام host را نمایش خواهد داد .

استفاده از ipconfig

ipconfig ، یکی از دستورات مفید به منظور بررسی وضعیت پیکربندی TCP/IP در کامپیوترهای سرویس دهنده و یا سرویس گیرنده ای است که بر روی آنان ویندوز نصب شده است . در یونیکس و لینوکس از دستور ifconfig در این رابطه استفاده می شود . در سیستم هائی که بر روی آنان ویندوز x9 و یا ME نصب شده است ، می توان از دستور winipcfg استفاده نمود .

استفاده از ipconfig

برای استفاده از دستور فوق، کافی است نام آن را از طریق پنجره command prompt تایپ نمود . عملکرد ipconfig و اطلاعاتی که در اثر اجرای آن نمایش داده خواهد شد به نوع سوئیچ استفاده شده ، بستگی دارد .

استفاده از ipconfig بدون سوئیچ

اطلاعات پیکربندی TCP/IP در ارتباط با هر یک از آداپتورهای موجود بر روی سیستم را نمایش خواهد داد:

- آدرس IP
- Subnet Mask
- gateway Default
- اطلاعات سرویس دهنده DNS
- Domain

دستور تایپ	خروجی
C:\> ipconfig	**Ethernet adapter MyLan1:** Connection-specific DNS Suffix . : IP Address. . . . . : 10.10.1.1 Subnet Mask . . . . . : 255.0.0.0 Default Gateway . . . . . : **PPP adapter Pars23:** Connection-specific DNS Suffix . : IP Address. . . . . : 10.1.1.216 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . : 10.1.1.216

دستور فوق ، اطلاعات مربوط به اتصالات از نوع PPP که از آنان در Dialup و VPN استفاده می شود را نیز نمایش خواهد داد .

استفاده از ipconfig به همراه سوئیچ all

علاوه بر نمایش اطلاعات اشاره شده در بخش قبل ، اطلاعات دیگری را نیز نمایش خواهد داد :

- آدرس سخت افزاری کارت شبکه (آدرس MAC)
- اطلاعات مربوط به DHCP

خروجی	دستور تایپ
Windows IP Configuration Host Name . . . . . : satanichell Primary DNS Suffix . . . . . : satanic Node Type . . . . . : Broadcast IP Routing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No DNS Suffix Search List. . . . . : satanic **Ethernet adapter MyLan1:** Connection-specific DNS Suffix . : Description . . . . . : D-Link DFE-680TX CardBus PC Card Physical Address. . . . . : 00-50-BA-79-DB-6A DHCP Enabled. . . . . : No IP Address. . . . . : 10.10.1.1 Subnet Mask . . . . . : 255.0.0.0 Default Gateway . . . . . : DNS Servers . . . . . : 127.0.0.1 **PPP adapter Pars23:** Connection-specific DNS Suffix . : Description . . . . . : WAN (PPP/SLIP) Interface Physical Address. . . . . : 00-53-45-00-00-00 DHCP Enabled. . . . . : No IP Address. . . . . : 10.1.1.216 Subnet Mask . . . . . : 255.255.255.255 Default Gateway . . . . . .: 10.1.1.216 DNS Servers . . . . . : x1.y1.z1.w1 x2.y2.z2.w2	**C:\> ipconfig /all**

سایر سوئیچ های دستور ipconfig : با استفاده از دستور ipconfig و برخی سوئیچ های آن (release ,renew) ، می توان اطلاعات مربوط به پیکربندی TCP/IP ارائه شده توسط سرویس دهنده DHCP را که در اختیار یک سرویس گیرنده قرار داده شده است را آزاد و یا آنان را مجددا" از سرویس دهنده درخواست نمود . فرآیند فوق به منظور تشخیص عملکرد صحیح سرویس دهنده DHCP در شبکه بسیار مفید و کارساز است . (آیا سرویس دهنده DHCP وظایف خود را به خوبی انجام می دهد ؟ آیا یک سرویس گیرنده قادر به برقراری ارتباط با سرویس دهنده DHCP به منظور درخواست و دریافت اطلاعات پیکربندی TCP/IP می باشد ؟) . دستور ipconfig دارای سوئیچ های مفید متعددی است که می توان با توجه به نوع خواسته خود از آنان استفاده نمود :

سوئیچ	عملکرد
/ release [adapter]	آدرس IP پیکربندی شده توسط DHCP را آزاد می نماید . در صورتی که سوئیچ فوق را به تنهائی و بدون مشخص نمودن adapter تایپ نمائیم،پیکربندی IP برای تمامی آداپتورهای موجود بر روی کامپیوتر، آزاد می گردد. در صورتی که قصد آزاد سازی اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم ، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد . (مثلا" ipconfig / release MyLan1)
/renew [adapter]	یک آدرس IP را بر اساس اطلاعات جدیدی که از طریق DHCP دریافت می نماید ، پیکربندی مجدد می نماید . در صورتی که سوئیچ فوق را به تنهائی و بدون مشخص نمودن adapter تایپ نمائیم،پیکربندی IP تمامی آداپتورهای موجود بر روی کامپیوتر، مجددا" انجام خواهد شد. در صورتی که قصد ایجاد مجدد اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم ، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد. (مثلا" ipconfig / renew MyLan1)
/ flushdn	حذف محتویات Dns Resolver Cache
/ registerdn	Refresh نمودن تمامی اطلاعات تولید شده توسط DHCP برای آداپتور و ریجستر نمودن اسامی Dns

نمایش محتویات Resolver Cache Dns	/ displaydns
نمایش تمامی Class ID DHCP مجاز برای آداپتور	/ showclassid [adapter]
تغییر ID DHCP Class	/setclassid [adapter] [classidtoset]

توضیحات :

- تشخیص نام آداپتور : نام آداپتور را می توان با کلیک (click Right) بر روی Network Neighborhood و انتخاب گزینه properties، از طریق پنجره Connections Network and Dial-up مشاهده نمود (اسامی آدپتورها ، نام آیکون ها می باشند) .
- مفهوم DNS Cache : زمانی که یک سیستم ، ترجمه (تبدیل نام host به آدرس) را از طریق یک سرویس دهنده DNS دریافت می نماید ، برای مدت زمان کوتاهی آن را در یک Cache ذخیره می نماید . در صورتی که مجددا" از نام استفاده شود ، پشته TCP/IP محتویات Cache را به منظور یافتن رکورد درخواستی بررسی می نماید . بدین ترتیب امکان پاسخگوئی سریعتر به درخواست ترجمه نسبت به حالتی که در خواست برای یک سرویس دهنده DNS ارسال می شود ، فراهم می گردد . با توجه به این که اندازه Cache نمی تواند از یک میزان منطقی و تعریف شده تجاوز نماید ، هر رکورد موجود در Cache پس از مدت زمانی خاص حذف می گردد. در صورت اعمال هرگونه تغییرات در DNS (مثلا" تغییر یک رکورد DNS) ، می توان با استفاده از دستور ipconfig/flushdns تمامی رکوردهای موجود در cache را حذف نمود . بدین ترتیب در صورت درخواست یک نام host ، با سرویس دهنده DNS مشورت می گردد و نتایج مجددا" در Cache ذخیره خواهند شد . دستور ipconfig / displaydns ، محتویات cache را نمایش خواهد داد. از اطلاعاتی که نمایش داده می شود ، می توان به منظور تشخیص این موضوع که آیا برای ترجمه نام به آدرس از Cache و یا سرویس دهنده DNS استفاده شده است ، کمک گرفت .
- موارد استفاده از دستور Ipconfig : از دستور فوق در مواردی که قصد تشخیص این موضوع را داریم که آیا سرویس دهنده DNS و DHCP در شبکه به درستی وظایف خود را انجام می دهند ، استفاده می شود(علاوه بر مشاهده اطلاعات پیکربندی TCP/IP) . مثلا" با استفاده از سوئیچ های release و renew ، می توان براحتی تشخیص داد که آیا در زمینه دریافت اطلاعات پیکربندی از یک سرویس دهنده DHCP مشکل خاصی وجود دارد

.از سوئیچ های مرتبط با DNS می توان به منظور اعمال تغییرات پیکربندی ، بهنگام سازی cache محلی و یا ریجستر نمودن اطلاعات پیکربندی جدید با یک سرویس دهنده DNS ، استفاده نمود .

- امکانات جانبی به همراه دستور ipconfig : با استفاده از سوئیچ all / اطلاعات متنوعی در رابطه با پیکربندی TCP/IP نمایش داده خواهد شد . در صورتی که حجم اطلاعات بگونه ای است که می بایست صفحه را scroll نمود ، می توان از More| به همراه دستور ipconfig استفاده نمود . در صورت تمایل می توان خروجی دستور ipconfig را در مقابل ارسال بر روی دستگاه استاندارد خروجی (صفحه نمایشگر) ، در یک فایل ذخیره نمود تا امکان بررسی سریعتر نتایج و رفع مشکل فراهم گردد.
(test1.txt < ipconfg /all)

همانگونه که اشاره گردید در سیتم هائی که از لینوکس و یا یونیکس استفاده می نمایند ، از دستور ifconfig استفاده می گردد. از دستور فوق برای نمایش اطلاعات پیکربندی IP و اعمال تغییرات لازم استفاده می شود .

دستور Ping

دستور Ping می تواند نقطه شروع مناسبی برای اشکال زدائی یک شبکه مبتنی بر TCP/IP باشد . از برنامه فوق برای تست وضعیت ارتباط بین دو سیستم موجود در شبکه استفاده می شود . این برنامه از پروتکل ICMP (اقتباس شده از Internet Message Protocol Control) به منظور مبادله بسته های اطلاعاتی با سیستم راه دور استفاده می کند (ICMP از پروتکل UDP برای حمل داده استفاده می نماید) .
برنامه Ping در ابتدا توسط Mike Muuss و با عملکردی ساده ، پیاده سازی گردید.
این برنامه از پروتکل ICMP به منظور ارسال پیام های UDP به یک آدرس (ECHO REQUEST) استفاده می نماید و 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 بر اساس آن Round-trip (ارسال یک درخواست و دریافت پاسخ) محاسبه می گردد .
ساختار بسته های اطلاعاتی ECHO REQUEST و ECHO REPLY در جدول زیر نشان داده شده است . از فیلد اطلاعاتی "نوع پیام " به منظور مشخص نمودن نوع پیام ، استفاده می شود . در صورتی 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 .

ساختار بسته های اطلاعاتی ECHO REQUEST و ECHO REPLY		
نوع پیام ICMP (صفر و یا هشت)	کد صفر	CheckSum
Identifier		Sequence number
data Optional		

استفاده از Ping

Ping دارای عملکردی بسیار ساده است . در ابتدا فیلد Sequence number مقدار صفر را خواهد گرفت و به ازای ارسال هر بسته اطلاعاتی، یک واحد به آن اضافه می شود . مقدار فیلد Identifier ، منحصر بفرد بوده تا امکان تشخیص بسته های اطلاعاتی برگردانده شده وجود داشته باشد (در مواردی که بیش از یک کاربر بطور همزمان از دستور Ping بر روی یک ماشین استفاده می نمایند) . در اکثر نسخه های یونیکس و لینوکس ، مقدار فیلد Identifier معادل 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 یافت :

- تمامی بسته های اطلاعاتی ارسالی ، مجددا" برگردانده می شوند . (بین سیستم ارسال کننده و دریافت کننده مشکل ارتباطی وجود ندارد) .
- برخی از بسته های اطلاعاتی ارسالی، توسط دریافت کننده برگردانده 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 نشاندهنده 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 و قادر به پاسخگوئی پیام های ECHO REQUEST در مدت زمان مشخص شده نمی باشد .

دستور Ping ، مدت زمان Round-trip بر حسب میلی ثانیه را محاسبه و نمایش می دهد .

برای محاسبه مدت زمان Round-trip ، برنامه ping زمان ارسال بسته اطلاعاتی را در فیلد Optional data قرار داده و پس از برگشت بسته اطلاعاتی، زمان ذخیره شده را با زمان جاری سیستم مقایسه نموده تا در نهایت مدت زمان رفت و 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 روتر موجود در مسیر بسته اطلاعاتی معمولا" به میزان یک ثانیه آن را کاهش می دهد .
در برخی موارد ممکن است در زمان ارسال درخواست های متوالی ping ، مدت زمان Round-trip کاهش پیدا نماید . این موضوع می تواند دلایل متعددی داشته باشد

- ماشین مقصد (و یا روتر gateway) در آن مقطع زمانی در جدول محلی ARP نمی باشد و مدت زمانی طول خواهد کشید (میلی ثاینه) تا arp آدرس سخت افزاری اولین بسته اطللاعاتی را بدست آورد .
- در صورتی که به همراه دستور ping در مقابل استفاده از آدرس IP از نام host استفاده شود ، ممکن است یافتن سرویس دهنده DNS که برنامه ping می بایست با آن ارتباط برقرار نماید(ترجمه نام host به آدرس IP) ، زمان خاص خود را داشته باشد .

در زمان استفاده از دستور Ping بهتر است که در ابتدا عملیات ping را در ارتباط با اینترفیس محلی و یا آدرس
(Loopback (IP: 127.0.0.1 شروع نمود . آدرس loopback در پشته TCP/IP استفاده شده و می توان از آن به منظور حصول اطمینان از صحت کارکرد پشته محلی ، استفاده نمود . آدرس فوق ، یک آدرس IP رزو شده است که امکان استفاده از آن در اینترنت وجود ندارد .

در صورتی که نمی توان آدرس IP سستم 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 .

استفاده از Ping در ویندوز

جدول زیر گرامر دستور Ping به همراه عملکرد برخی از سوئیچ های متداول آن را نشان می دهد :

گرامر دستور Ping در ویندوز	
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list	
سوئیچ	عملکرد
-t	به صورت پیوسته عملیات Ping را انجام می دهد. برای توقف برنامه ping می توان از کلیدهای CTRL+C استفاده نمود .
-a	ترجمه آدرس به نام را انجام می دهد
-n count	تعداد بسته های اطلاعاتی ICMP ECHO REQUEST ارسالی را مشخص می نماید .
-l size	اندازه بافر را ارسال می نماید.
-i TTL	مقدار TTL را مشخص می نماید .
-w timeout	مدت زمان انتظار پاسخ برحسب میلی ثانیه

نحوه استفاده از دستور Ping :

دستور تایپ	خروجی
C:\>ping www.shabgard.org	Pinging www.shabgard.org [195.219.180.15] with 32 bytes of data: Reply from 195.219.180.15: bytes=32 time=421ms TTL=238 Reply from 64.233.187.99: bytes=32 time=430ms TTL=238 Reply from 64.233.187.99: bytes=32 time=431ms TTL=238 Reply from 64.233.187.99: bytes=32 time=430ms TTL=238 Ping statistics for 195.219.180.15: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 421ms, Maximum = 431ms, Average = 428ms

توضیحات :

- چهار بسته اطلاعاتی ارسال شده است که همان چهار بسته نیز دریافت شده اند (در زمان انتقال، هیچیک از بسته های اطلاعاتی گم نشده اند)
- زمان پاسخ حدودا" 430 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 ارسال کننده درست است ؟ برای 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 ping از نام host استفاده نمائید . ping ، قبل از ارسال 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 تصور آن را دارید ، می بایست پیکربندی سیستم خود را بررسی نمائید . در چنین مواردی ممکن است شما کامپیوتر خود را بگونه ای پیکربندی نموده اید که از یک آدرس IP خاص استفاده نماید ولی در سرویس دهنده DNS ، به کامپیوتر شما یک آدرس IP دیگر مرتبط 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 ، ping نمائید . 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 Gateway ، روتر و یا دستگاهی دیگر است که Subnet شما را به سایر شبکه ها متصل می نماید. در صورت عدم امکان ping نمودن Gateway Default ، دو احتمال 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 اطلاعاتی در Local Subnet است ، استفاده می نمائید . **احتمال دوم** : ممکن است خود gateway Default دارای مشکل باشد . برای اطمینان از این موضوع ، می توان از طریق یک سیستم دیگر موجود در شبکه ، Default Gateway را 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 برقرار شده 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

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 Death Ping of 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 مجاز می باشند . در صورتی که نرم افزار موجود بر روی سیستم مقصد به درستی Patch نشده باشد ، بسته های اطلاعاتی ارسالی توسط مهاجمان دریافت و بخش عمده ای از حافظه را اشغال نموده و می تواند سرریز حافظه را بدنبال داشته باشد . مدیران شبکه می بایست یک محیط ایمن به منظور استفاده از ping را در شبکه فراهم نموده تا امکان تحقق چنین حملاتی در شبکه وجود نداشته باشد .

در صورتی که نتوان یک کامپیوتر راه 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 : بروز اشکال در هر یک از دستگاه های موجود در مسیر ارتباطی نظیر هاب ، سوئیچ ، روتر و یا Gateway Default . به همین دلیل ، می بایست همواره یک طرح کامل از شبکه به همراه جزئیات مربوطه وجود داشته باشد تا در صورت 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 .

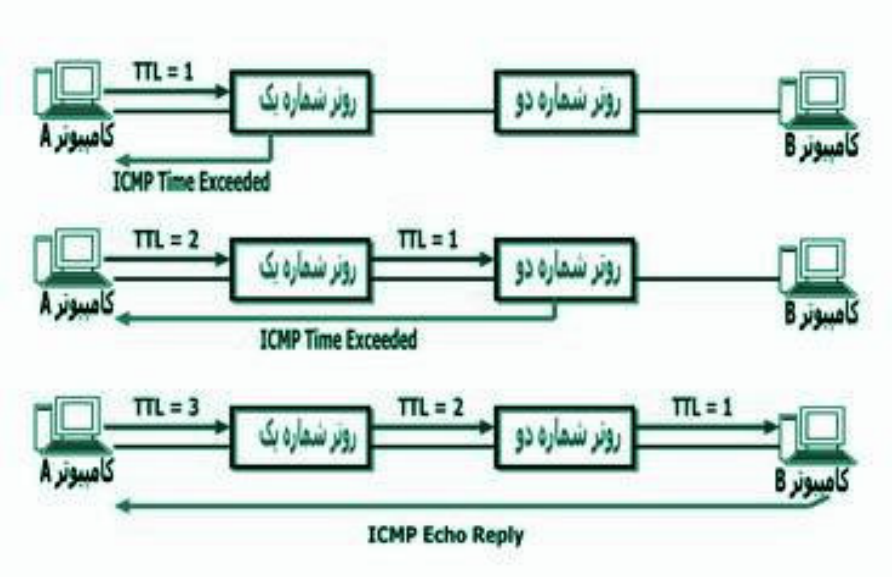
موارد استفاده از دستور tracert

- عدم امکان ping نمودن یک کامپیوتر موجود در خارج از Gateway پیش فرض . با استفاده از دستور فوق ، می توان کامپیوترها و روترهای موجود در مسیر یک بسته اطلاعاتی تا رسیدن به مقصد نهائی را مشاهده نمود . بدین ترتیب امکان مشاهده محلی که از آن نقطه به بعد امکان حرکت بسته اطلاعاتی وجود ندارد ، فراهم می گردد .

- در صورتی که امکان حرکت بسته های اطلاعاتی از مبداء به مقصد وجود نداشته باشد و یا زمان پاسخ دستور ping زمانی نامعقول و طولانی باشد .
- آگاهی از محل توقف یک بسته اطلاعاتی در شبکه

نحوه عملکرد دستور tracert

دستور فوق از فیلد TTL مربوط به IP در Request ICMP Echo و پیام های ICMP Time Exceeded به منظور تعیین مسیر مبداء تا مقصد یک بسته اطلاعاتی استفاده می نماید . عملکرد این دستور نیز مشابه ping است و وی نیز از پیام های مبتنی بر ICMP برای یافتن هر یک از دستگاه های موجود در مسیر یک بسته اطلاعاتی ، استفاده می نماید . برای تشخیص مسیر حرکت ، به TTL موجود در بسته اطلاعاتی یک مقدار اولیه نسبت داده می شود . TTL ، یک عدد صحیح است که حداکثر تعداد hop (گره و یا روتر) را که یک بسته اطلاعاتی در مسیر خود با آنان برخورد می نماید را مشخص می نماید (قبل از این که توسط IP دور انداخته شود). مقدار TTL در ابتدا یک خواهد بود و هر روتر و دستگاه موجود در مسیر بسته اطلاعاتی ، یک واحد به آن اضافه می نماید .
بدین ترتیب برنامه tracert قادر به دریافت پیام TIME_EXCEEDED ICMP از هر یک از روترها و یا سایر دستگاه های موجود در مسیر یک بسته اطلاعاتی می باشد .
شکل زیر نحوه عملکرد دستور tracert را نشان می دهد .



همانگونه که در شکل فوق مشاهده می گردد ، کامپیوتر A یک مجموعه از پیام های ICMP ECHO REQUEST را تولید و آنان را برای کامپیوتر B ارسال می نماید. زمانی که اولین بسته اطلاعاتی ارسال می شود ، مقدار TTL یک خواهد بود و در

روتر شماره یک مقدار آن صفر شده و یک پیام TIME_EXCEEDED ICMP ، برای کامپیوتر A ارسال می گردد . کامپیوتر A مجددا" یک بسته اطلاعاتی ICMP دیگر را ارسال می نماید . ولی این مرتبه مقدار TTL آن دو در نظر گرفته می شود . در چنین حالتی روتر اول ، بسته اطلاعاتی را عبور داده و یک واحد از مقدار TTL کم می نماید و آن را برای روتر دوم ارسال می نماید . (در این مقطع مقدار TTL=1 شده است) . روتر دوم مقدار TTL را بررسی نموده و از آن یک واحد کم خواهد کرد . با توجه به این که مقدار TTL=0 صفر شده است ، مجددا" یک پیام TIME_EXCEEDED ICMP برای کامپیوتر A ارسال می گردد . زمانی که ICMP ECHO REQUEST به کامپیوتر B می رسد ، وی یک ICMP Echo Reply را برمی گرداند . بدین ترتیب ، کامپیوتر A قادر به تشخیص تعداد hop موجود در مسیر خواهد بود.

استفاده از دستور tracert

جدول زیر گرامر دستور tracert به همراه عملکرد برخی از سوئیچ های متداول آن را نشان می دهد :

گرامر دستور tracert در ویندوز	
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name	
سوئیچ	عملکرد
-d	نام host را به آدرس IP ترجمه نمی نماید .
-h maximum_hops	حداکثر تعداد hop برای جستجوی مقصد را مشخص می نماید .
-w timeout	مدت زمان انتظار برای دریافت پاسخ بر حسب میلی ثانیه را مشخص می نماید .

نحوه استفاده از دستور tracert :

دستور تایپ	خروجی
C:\>tracert www.shabgard.org	Tracing route to www.shabgard.org [195.219.180.15] over a maximum of 30 hops:

1 180 ms 170 ms 191 ms x1.y1.z1.w1 2 201 ms 190 ms 190 ms x2.y2.z2.w2 3 201 ms 180 ms 190 ms x3.y3.z3.w3 4 * 217.220.96.145 reports: **Destination net unreachable.** Trace complete.	

توضیحات :

- در مواردی که در مسیر یک بسته اطلاعاتی مشکل خاصی ایجاد شود و یا پیام ICMP Time Exceeded برگردانده نشود ، در خروجی علامت "ستاره" نشان داده خواهد شد (در سه ستونی که معمولا" زمان round-trip را نمایش می دهند) . در چنین مواردی یک پیام timed out Request در قسمت سمت راست نمایش داده می شود .
- در برنامه اولیه tracert مقدار پورت در هدر UDP ، یک پورت UNREACHABLE در نظر گرفته می شد . بنابراین زمانی که بسته اطلاعاتی ICMP به مقصد نهائی خود می رسد ، یک پیام ICMP DESTINATION UNREACHABLE توسط کامپیوتر مقصد برگردانده می شود .
- در صورتی که آخرین گره مشاهده شده در خروجی دستور tracert مقصد نهائی باشد ، تمامی گره ها و یا روترهای موجود در مسیر نمایش داده شده اند

این مقاله هم به پایان رسید امیدوارم مطالب درست وکاملی را به شما گفته باشم ☻ ☺

در دو چشمش گناه مي خنديد
در گذرگاه آن لبان خموش
شعله يي بي پناه مي خنديد
شرمناك و پر از نيازي گنگ
با نگاهي كه رنگ مستي داشت
در دو چشمش نگاه كردم و گفت
بايد از عشق حاصلي برداشت
سايه يي روي سايه يي خم شد
در نهانگاه رازپرور شب
نفسي روي گونه يي لغزيد
بوسه يي شعله زد ميان دو لب
سحر گاهي زني دامن كشان رفت
پريشان مرغ ره گم كرده اي بود
به چشمي خيره شد شايد بيابد
نهانگاه اميد و آرزو را
دريغا آن دو چشم آتش افروز
به دامان گناه افكند او را
به او جز از هوس چيزي نگفتند
در او جز جلوه ظاهر نديدند
به هرجا رفت در گوشش سرودند
كه زن را بهر عشرت آفريدند
شبي در دامني افتاد و ناليد
شبي نا گه سر آمد انتظارش
لبش در كام سوزاني هوس ريخت

چرا آن مرد بر جانش غضب کرد ؟
چرا بر ذره هاي جامش آويخت ؟
کنون اين او و اين خاموشي سرد
نه پيغامي نه پيك آشنايي
گنه کردم گناهي پر ز لذت
درآغوشي که گرم و آتشين بود
گنه کردم ميان بازواني
که داغ و کينه جوي و آهنين بود
در آن خلوتگه تاريك و خاموش
گنه کردم چشم پر ز رازش
دلم در سينه بي تابانه لرزيد
ز خواهش هاي چشم پر نيازش
در آن خلوتگه تاريك و خاموش
پريشان در کنار او نشستم
لبش بر روي لبهايم هوس ريخت
ز اندوه دل ديوانه رستم
فروخواندم به گوشش قصه عشق
ترا مي خواهم اي جانانه من
ترا مي خواهم اي آغوش جانبخش
ترا اي عاشق ديوانه من
هوس در ديدگانش شعله افروخت
شراب سرخ در پيمانه رقصيد
تن من در ميان بستر نرم
بروي سينه اش مستانه لرزيد
گنه کردم گناهي پر ز لذت
کنار پيکري لرزان و مدهوش
خداوندا چه مي دانم چه کردم
در آن خلوتگه تاريك و خاموش

تو را مي خواهم و دانم که هرگز
به کام دل در آغوشت نگيرم
تويي آن آسمانه صاف و روشن
من کنج قفس مرغي اسيرم

©CopyRight®

Author: Satanic Soulful
E-Mail: Satanic.Soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Developed In:Satanic Digital Network Security ™
Special TNX 2 :Hell Hacker – Collector – S_hahroo_Z
Research By:5/-\t4N1C

For More Information Go to Http://Hack-er.cjb.net/

My Deram Is All Day For Girl Is Dark&Ominous♀