از آنجايي كه در دنياي مجازي اينترنت و به خصوص دنياي امنيت يكي از مهمترين قسمتها بخش پايه شبكه و بخصوص TCP/IP مي باشد ما بر آن شديم تا در اين سري مقالات در خصوص TCP/IP و تا حدودي osi مختصري بپردازيم پيشاپيش هر قصور و كمبودي را به بزرگواري خودتان بر اين شاگرد ناچيز ببخشيد .

OSI چيست ؟

OSI (Open System Interconnection) يك مدل مرجع براي ارتباط بين دو كامپيوتر مي باشد كه در سال ۱۹۸۰ طراحي گرديده است. هر چند امروزه تغييراتي درآن به وجود آمده اما هنوز هم كاربردهاي فراواني در جاهاي مختلف اينترنت و به خصوص در پايه هاي شبكه دارد.

اين مدل بر اساس لايه بندي قراردادهاي برقراري ارتباط كه همزمان روي دو سيستم مرتبط اجرا شده اند پايه ريزي شده است كه اين امر بسيار سرعت و دقت ارتباط را افزايش مي دهد و اين قراردادها بصورت طبقه طبقه در هفت لايه تنظيم شده اند كه در زير بررسي خواهند شد. (شكل ۱)

مدل مرجع osi	
Application	لايه كاربرد
Presentation	لايه ارائه
Session	لايه جلسه
Transport	لايه انتقال
Network	لايه شبكه
Data link	لايه پيوند داده ها
Physical	لايه فيزيكي

شكل ۱: لايه هاي مدل OSI

بررسي هفت لايه OSI :

لايه فيزيكي :

اين لايه كه تنها تشكيل شده از سخت افزار مي باشد و قراردادهاي سخت افزاري در آن اجرا مي شود وظيفه انتقال نهايي اطلاعات را دارد كه اين انتقال بصورت سيگنال و به صورت صفرو يك مي باشد

لايه پيوند داده ها :

در اين لايه اطلاعات ، كشف خطا و اصلاح مي شوند و بدون خطا و به صورت مطمئن به سوي مقصد ارسال مي شوند .وظيفه ديگر اين لايه مطمئن شدن از رسيدن اطلاعات به مقصد است كه اين كار توسط بيتهاي (Parity check , checksum ,crc) انجام مي پذيرد .كه در صورت بروز خطا مجددا اطلاعات ارسال خواهند شد .

لايه شبكه :

و اما پيچيده ترين لايه يعني لايه شبكه كه در آن قراردادهاي شبكه بندي تعريف شده است . وظيفه اين لايه انتقال تكنولوژي برقراري ارتباط براي ديگر شبكه هاي مستقل است كه اين امر اين امكان را به osi مي دهد كه بتواند در زير شبكه هاي مختلف فعاليت كند .

لايه انتقال :

در اين لايه قبل از ارسال اطلاعات يك بسته به سمت مقصد فرستاده مي شود تا مقصد را براي دريافت اطلاعات آماده كند . همچنين اين لايه وظيفه تكه تكه كردن بسته ها ، شماره گذاري آنها و ترتيب و نظم دهي آنها را بر عهده دارد. كه البته بسته ها در طرف گيرنده دوباره در همين لايه نظم دهي و قابل استفاده براي لايه هاي بالاتر خواهند شد.

لايه جلسه :

در اين لايه بر كارهايي از قبيل زمان ارسال و دريافت بسته ها مقدار رسيده و مقدار مانده از بسته ها نظارت مي شود كه به مديرت بسته ها بسيار كمك مي كند .

لايه ارائه :

در اين لايه استانداردهاي رمز نگاري و فشرده سازي اطلاعات تعريف شده است كه اين لايه در امنيت بسيار مهم مي باشد .

لايه كاربرد :استانداردهاي ارتباط بين نرم افزارهاي شبكه در اين لايه قرار دارد كه مي توان از :

MHS VT CMIP FTAM نام برد.

« Internet protocol /Transmission Control Protocol » TCP/IP

TCP/IP چيست ؟

TCP/IP مجموعه قراردادهايي هستند كه در جهت اتصال كامپيوتر ها در شبكه مورد استفاده قرار مي گيرند. وبه تعريف ديگر قرارداد كنترل انتقال اطلاعات مي باشد .

مقايسه با osi: (شكل۲)

مدل مرجع osi	مدل چهار لايه TCP/IP
لايه كاربرد	لايه كاربرد
لايه ارائه	
لايه جلسه	لايه انتقال
لايه انتقال	
لايه شبكه	لايه شبكه
لايه پيوند داده ها	لايه واسطه شبكه
لايه فيزيكي	

همانطور كه از شكل پيداست TCP/IP از چهار لايه تشكيل شده كه در زير به صحبت در مورد چهار لايه TCP/IP مي پردازيم .

لايه واسط شبكه :

در اين لايه تمام استانداردهاي سخت افزاري و انواع پروتكل شبكه تعريف شده كه خاصيت بزرگ اين لايه اين موضوع مي باشد كه در آن مي توان بين نرم افزار و سخت افزار شبكه ارتباط برقرار كرد.

لايه شبكه :

در اين لايه پروتكل IP آدرس دهي و تنظيم مي شود .(توضيحات در قسمت IP) و همچنين ديگر پروتكل ها مانند ARP,ICMP,BOOTP كه در اين ميان نقش هيچكدام به اندازه IP , ICMP مهم نيست در كل وظيفه اين لايه دادن اطلاعات در مورد شبكه و آدرس دهي در آن مي باشد كه مسير يابها از آن بسيار استفاده مي كنند .

لايه انتقال :

ابتدايي ترين وظيف اين لايه آگاهي از وضعيت بسته ها مي باشد كه بسيار مهم نيز هست .

و در مرحله بعد وظيفه اين لايه انتقال اطلاعاتي مي باشد كه نياز به امنيت ندارند و سرعت براي آنها مهم تر است

لايه كاربرد :

اين لايه داراي امكانات زيادي براي هنر نمايي متخصصان مي باشد.

در اين لايه برنامه هاي كاربردي قرار دارند و در كل اين لايه لايه ي نرم افزارهاي شبكه مي باشد و همچنين لايه پروتكل هاي نرم افزاري نيز مي باشد .

از مهم ترين نكات در خصوص اين لايه قرارداشتن : انتقال فايل (FTP) و مديريت پست (SMTP) و بقيه برنامه هاي كاربردي مي باشد .

پروتكل اينترنت IP

حتما همه شما عزيزان واقف به اين موضوع هستيد كه IPيكي از مهمترين قسمتهاي TCP/IP و شايد بتوان گفت مهمترين قسمت آن زيرا تقريبا شما براي هر كاري نياز به آن خواهيد داشت لذا بسيار ضروري و حياتي مي باشد كه شما اطلاعات خود را در زمينه اين مهم افزون كنيد .

IPيك آدرس عددي است كه براي ارتباط با شبكه به هر ماشيني در شبكه اختصاص داده مي شود (چون IPبراي وسايلي از قبيل ROUTERو MODEM و LAN و ... استفاده مي شود ما اصطلاحا به جاي نام بردن تك تك آنها همه را ماشين ميناميم)

« IP شما نسبت به نوع اتصال شما متغيير و يا ثابت مي باشد. »

وظيفه IPچيست ؟

وظيفه پروتكل IP حمل و تردد بسته هاي حاوي اطلاعات و همچنين مسير يابي آنها از مبدا تا مقصد است

اساس كار پروتكل IPچيست ؟

IP پس از دريافت اطلاعات از TCP شروع به قطعه قطعه كردن آن به قطعه هاي كوچك به اسم FRAGMENT مي نمايد، پس از اين مرحله براي هر FRAGMENT يك بسته IP مي سازد كه حاوي اطلاعات مورد نياز بسته براي حركت در طول شبكه مي باشد و بسته IP را به بسته TCP اضافه مي كند

و شروع به ارسال بسته هاي تيكه تيكه شده(FRAGMENT) مي نمايد حال مسير يابها بر اساس تنظيمات قسمت IP بسته ها را به مقصد خود هدايت مي كنند و آن را داخل زير شبكه ها هدايت مي كنند

خصوصيات IP :

بسته IP حد اكثر ٦٤ كيلوبايت فضا را اشغال خواهد كرد و بيشتر از آن نمي تواند باشد ولي موضوع جالب اينجاست كه در حالت عادي حجم بسته حدود ١٦٠٠ بايت بيشتر نمي شود

« بعدها يك حمله d.o.s بر مبناي همين موضوع طراحي شد »

IP در تمامي سيستم هاي عامل با ساختار استانداردي كه دارد به درستي كار مي كنند و نياز به هيچ نوع سخت افزار ندارد .

بررسي ساختار بسته ساخته شده توسط پروتكل IP

بسته IP ساخته شده از تعدادي فيلد مجزا مي باشد كه هر كدام اطلاعاتي را در خود دارند كه در زمان مورد نياز اين اطلاعات از داخل بسته ها استخراج مي شود و مورد استفاده قرار مي گيرد اين اطلاعات شامل مواردي مثل :آدرس IP فرستنده . آدرس IP گيرنده و ..... مي باشد

بررسي فيلدها :

فيلد version:

وظيفه مشخص كردن نوع پروتكل IP را بر عهده دارد (در حال حاضر از دو version ٤و٦ استفاده مي شود)

اندازه فيلد :چهار بيت

فيلد :IHL

وظيفه اين فيلد نگهداري اندازه قسمت بالايي بسته در خود مي باشد كه از آن براي تعيين مرز بين اطلاعات و محتويات بسته IP استفاده مي شود .

اندازه فيلد : ٤ بيت

فيلد TYPE OF SERVICE:

دراين فيلد نوع سرويس انتقال تعيين مي شود : ((كم سرعت و مطمئن))و ((پر سرعت و نامطمئن))

اندازه فيلد : هشت بايت

فيلد TOTAL LENGTH :

در اين فيلد اندازه كل بسته IP قرار دارد كه شامل قسمت سر آيند و ناحيه داده مي باشد كه همانطور كه گفته شد مي تواند ٦٥٥٣٥ بايت باشد .

اندازه فيلد : ١٦ بيت

فيلد FRAGMENT OFFSET :

اين قيلد خود به سه بخش تقسيم مي شود :

١- بيت (DF(DON'T FRAGMENT: اگر اين بيت ١ باشد هيچ مسير يابي حق شكستن اين بسته را ندارد

٢- بيت (MF(MORE FEAGMENT: اگر اين بيت ٠ بود به اين معني مي باشد كه اين قطعه آخرين قطه ارسال شده مي باشد

٣- FRAGMENT OFFSET

در اين قسمت شماره قطعه هاي شكسته شده قرار دارد و چون اندازه اين فيلد ١٣ بيت مي باشد اطلاعات مي توانند تا ٨١٩٢ قطعه شكسته شوند (اندازه هر قطعه به غير از قطعه آخري بايد ضريبي از ٨ باشد)

فيلد TIME TO LIVE:

همانطور كه مي دانيد در اين فيلد زمان سرگرداني بسته مشخص مي شود و اين به معني مي باشد كه اين بسته مي تواند از چند مسير ياب عبوركند كه حداكثر آن ٢٥٥مي باشد . اين فيلد يك نعمت بزرگ مي باشد

اندازه فيلد :٨ بيت

فيلد PROTOCOL:

در اين فيلد شماره پروتكلي كه قرار است بسته به آن برسد مشخص مي شود

فيلد : HEADER CHECKSUM:

وظيف كشف خطا را بر عهده دارد

فيلد SOURCE ADDRESS :

اين فيلد فيلد بسيار مهمي مي باشد چون در آن آدرس مبدا موجود مي باشد برنامه هاي فيلترنيگ و فايروالها بسيار از اين فيلد استفاده مي كنند .

فيلد DESTINATION ADDRESS:

در اين فيلد هم آدرس IP مقصد موجود مي باشد

فيلد OPTION :

اين فيلد يك فيلد خالي مي باشد كه در آن هر توضيحاتي به صورت دلخواه مي توان نوشت

فيلد PAYLOAD:

در اين فيلد داده ها بين لايه هاي مختلف رد و بدل مي شود البته اين امر از لايه هاي بالا به سمت لايه هاي پائينتر صورت مي گيرد

نكاتي جالب در مورد IP

آدرس هاي ويژه :

اين آدرسها نمونه هاي از آدرس هاي IP خاص هستند كه از قبل براي مقاصد خاصي در نظر گرفته شده اند و در تعريف شبكه نمي توان از آنها به عنوان IP براي ماشينها استفاده كرد .

0.0.0.0

از اين آدرس در مواردي استفاده مي شود كه ماشين ميزبان از IP خود بي اطلاع است .البته اگر از اين آدرس به عنوان آدرس فرستنده استفاده شود هيچ جوابي براي فرستنده پس فرستاده نمي شود .

HostId.0

اين آدرس براي زماني است كه از آدرس خود در زيرشبكه بي اطلاع باشيم

255.255.255.255

از اين آدرس براي ارسال پيامهاي به صورت عمومي و فراگير در شبكه استفاده مي شود البته با استفاده از اين آدرس مي توان در زير شبكه خود پيام فراگير ارسال كرد .

NetId.255

از اين آدرس براي ارسال پيامهاي فراگير در ديگر شبكه ها از خارج از آنها استفاده مي شود .البته اين سرويس تقريبا در بيشتر اوقات از سوي مديران شبكه غير فعال مي شود .

در ادامه مباحث tcp/ip به بررسي ساختار فيلدهاي بسته tcp و udp وicmp .... و چند پروتكل مشهور خواهيم پرداخت
بسته tcp نيز همانند ip تشكيل شده از تعدادي فيلد مي باشد كه توضيحاتي در مورد شماره پورت مقصد شماره پورت مبدا و .... را در خود دارد حال به بررسي اين فيلدهاي مهم مي پردازيم .

فيلدهادر بسته هاي tcp

فيلد source port :
اين فيلد كه مقداري برابر ١٦ بيت دارد آدرس پورت(پروتكل) مبدا را در خود دارد با استفاده از اين فيلد تقريبا مي توان نوع داده هاي ارسالي را فهميد

فيلد destination :
در اين فيلد آدرس پورتي كه اطلاعات در مقصد بايد تحويل آن داده شود موجود مي باشد
اين فيلد تعيين مي كند كه ما اطلاعات را براي چه پورتي ارسال مي كنيم كه البته در بيشتر موارد اطلاعات براي پروتكلهاي استاندارد ارسال مي شود براي مثال پورت ٨٠ به صورت استاندارد پروتكل http را در خود دارد .

فيلد sequence number
اين فيلد داراي عددي است كه نشان دهنده تعداد بايتهاي ارسال شده از داده ها است كه اين عدد با احتساب داده هاي بسته جاري در فيلد قرار مي گيرد براي مثال اگر داخل فيلد عدد ٢٢٢٢٢٢ قرار بگيرد يعني پس از ارسال بسته جاري ٢٢٢٢٢٢بايت از داده ها ارسال شده است

فيلد acknowledgment number :
همانطور كه از اسم اين فيلد پيداست فيلدي است براي تصديق كردن مقدار اطلاعات دريافت شده از طرف گيرنده براي مثال اگر در اين فيلد كه ظرفيت آن ٣٢ بيت مي باشد عدد ١٠٠٠٠٠١ قرار داشته باشد به اين معني است كه گيرنده دريافت اطلاعات تا اين بيت را تائيد كرده و منتظر دريافت بقيه اطلاعات مي باشد

فيلد tcp header length:
در اين فيلد نيز عددي وجود دارد كه مرز بين داده ها و سر آيند بسته را مشخص مي كند
سر آيند به قسمتي گفته مي شود كه شامل فيلدهاي TCP مي باشد

فيلد Windows size :
در اين فيلد مقدار فضايي كه در طرف گيرنده خالي مانده است قرار دارد
كاربرد اين فيلد به اين صورت است كه مقداري كه در اين فيلد قرار دارد (مقدار فضاي خالي بافر گيرنده) با مقدار داده اي كه براي ارسال آماده است مقايسه مي شود اگر بافر گيرنده فضاي كافي داشته باشد داده ها ارسال مي شود و در غير اينصورت منتظر مي ماند تا بافر گيرنده خالي شود و بعد اقدام به ارسال داده ها مي كند

فيلد checksum :
اين فيلد كه فضايي ١٦ بيتي را اشغال مي كند حاوي كد خطاهاي به وجود آمده در ارسال يا دريافت اطلاعات مي باشد

فيلد Tcp segment length:
اين فيلد مقدار كل بسته را بر حسب بايت در خود دارد

فيلد urgent pointer :
در اين فيلد يك عدد كه در اصل يك كد شبيه به كد وقفه ها است قرار دارد كه در مواقع ضروري ارسال مي شود

فيلد option :
اين فيلد يك نعمت بزرگ مي باشد در مواقعي كه حجم بسته ضريبي از چهار نشود از اين قسمت با داده هاي بي ارزش استفاده مي شود تا مقدار ضريبي از چهار شود

بيت Urg :
اين فيلد نشان دهنده وضعيت فيلد urgent pointer مي باشد
طرز عملكرد اين فيلد١ بايتي به اين شكل مي باشد كه اگر مقدار آن ١ باشد به اين معني است كه فيلد urgent pointer بايد مورد ارزيابي قرار گيرد و اگر مقدار آن صفر باشد نسبت به آن فيلد بي تفاوت است

بيت ack:
اگر در اين فيلد مقدار ١ قرار گيرد دليل بر اعتبار فيلد acknowledgment مي باشد.

بيت PSH :
اين بيت براي جداسازي بسته هاي حياطي و مهم مورد استفاده قرار مي گيرد
اين فيلد به گيرنده نشان مي دهد كه بسته حاوي آن بايد سريعا بافر شود و به برنامه كاربردي تحويل داده شود
براي مثال در telnet

بيت RST :
اين بيت براي قطع ارتباط مورد استفاده قرار مي گيرد اما قطع ارتباط در اين صورت يكطرف خواهد بود و ارسال داده ها ناتمام خواهد ماند و طرز كار آن به اين صورت است كه اگر حاوي ١ باشد ارتباط را بدون اجازه و خبر دادن به طرف مقابل قطع مي كند

بيت syn :
اين بيت يكي از مهمترين قسمتهاي بسته tcp مي باشد چون نقش برقراري ارتباط را بر عهده دارد

و اما آخرين بيت كه بيت FIN مي باشد :
اين بيت تقريبا به معناي خداحافظي مي باشد
موقعي كه يكي از طرفين داده اي براي ارسال نداشته باشد اين بيت را ١ مي كند و اين بدان معناست كه اين آخرين بسته ارسالي مي باشد وبعد از ارسال بسته ارتباط به صورت يكطرفه قطع خواهد شد .