

از آنجایی که در دنیای مجازی اینترنت و به خصوص دنیای امنیت یکی از مهمترین قسمتها بخش پایه شبکه و بخصوص TCP/IP می باشد ما بر آن شدیم تا در این سری مقالات در خصوص TCP/IP و تا حدودی OSI مختصری بهرذایم پیشاپیش هر قصور و کمبودی را به بزرگواری خودتان بر این شاگرد ناچیز ببخشید .

OSI چیست ؟

OSI (Open System Interconnection) یک مدل مرجع برای ارتباط بین دو کامپیوتر می باشد که در سال ۱۹۸۰ طراحی گردیده است. هر چند امروزه تغییراتی در آن به وجود آمده اما هنوز هم کاربردهای فراوانی در جاهای مختلف اینترنت و به خصوص در پایه های شبکه دارد.

این مدل بر اساس لایه بندی قراردادهای برقراری ارتباط که همزمان روی دو سیستم مرتبط اجرا شده اند پایه ریزی شده است که این امر بسیار سرعت و دقت ارتباط را افزایش می دهد و این قراردادها بصورت طبقه طبقه در هفت لایه تنظیم شده اند که در زیر بررسی خواهند شد. (شکل ۱)

مدل مرجع OSI	
Application	لایه کاربرد
Presentation	لایه ارائه
Session	لایه جلسه
Transport	لایه انتقال
Network	لایه شبکه
Data link	لایه پیوند داده ها
Physical	لایه فیزیکی
شکل ۱: لایه های مدل OSI	

بررسی هفت لایه OSI :

لایه فیزیکی :

این لایه که تنها تشکیل شده از سخت افزار می باشد و قراردادهای سخت افزاری در آن اجرا می شود وظیفه انتقال نهایی اطلاعات را دارد که این انتقال بصورت سیگنال و به صورت صفرو یک می باشد

لایه پیوند داده ها :

در این لایه اطلاعات ، کشف خطا و اصلاح می شوند و بدون خطا و به صورت مطمئن به سوی مقصد ارسال می شوند .وظیفه دیگر این لایه مطمئن شدن از رسیدن اطلاعات به مقصد است که این کار توسط بیتهای (crc , checksum , Parity check) انجام می پذیرد .که در صورت بروز خطا مجددا اطلاعات ارسال خواهند شد .

لایه شبکه :

و اما پیچیده ترین لایه یعنی لایه شبکه که در آن قراردادهای شبکه بندی تعریف شده است . وظیفه این لایه انتقال تکنولوژی برقراری ارتباط برای دیگر شبکه های مستقل است که این امر این امکان را به OSI می دهد که بتواند در زیر شبکه های مختلف فعالیت کند .

لایه انتقال :

در این لایه قبل از ارسال اطلاعات یک بسته به سمت مقصد فرستاده می شود تا مقصد را برای دریافت اطلاعات آماده کند . همچنین این لایه وظیفه تکه تکه کردن بسته ها ، شماره گذاری آنها و ترتیب و نظم دهی آنها را بر عهده دارد. که البته بسته ها در طرف گیرنده دوباره در همین لایه نظم دهی و قابل استفاده برای لایه های بالاتر خواهند شد.

لایه جلسه :

در این لایه بر کارهایی از قبیل زمان ارسال و دریافت بسته ها مقدار رسیده و مقدار مانده از بسته ها نظارت می شود که به مدیریت بسته ها بسیار کمک می کند .

لایه ارائه :

در این لایه استانداردهای رمز نگاری و فشرده سازی اطلاعات تعریف شده است که این لایه در امنیت بسیار مهم می باشد .

لایه کاربرد : استانداردهای ارتباط بین نرم افزارهای شبکه در این لایه قرار دارد که می توان از :

FTAM CMIP MHS VT نام برد.

« Internet protocol /Transmission Control Protocol » TCP/IP

TCP/IP چیست ؟

TCP/IP مجموعه قراردادهایی هستند که در جهت اتصال کامپیوتر ها در شبکه مورد استفاده قرار می گیرند. و به تعریف دیگر قرارداد کنترل انتقال اطلاعات می باشد .

مقایسه با osi: (شکل ۲)

مدل مرجع osi	مدل چهار لایه TCP/IP
لایه کاربرد	لایه کاربرد
لایه ارائه	
لایه جلسه	لایه انتقال
لایه انتقال	
لایه شبکه	لایه شبکه
لایه پیوند داده ها	لایه واسطه شبکه
لایه فیزیکی	

همانطور که از شکل پیداست TCP/IP از چهار لایه تشکیل شده که در زیر به صحبت در مورد چهار لایه TCP/IP می پردازیم .

لایه واسطه شبکه :

در این لایه تمام استانداردهای سخت افزاری و انواع پروتکل شبکه تعریف شده که خاصیت بزرگ این لایه این موضوع می باشد که در آن می توان بین نرم افزار و سخت افزار شبکه ارتباط برقرار کرد.

لایه شبکه :

در این لایه پروتکل IP آدرس دهی و تنظیم می شود . (توضیحات در قسمت IP) و همچنین دیگر پروتکل ها مانند ARP,ICMP,BOOTP که در این میان نقش هیچکدام به اندازه ICMP , IP مهم نیست در کل وظیفه این لایه دادن اطلاعات در مورد شبکه و آدرس دهی در آن می باشد که مسیر یابها از آن بسیار استفاده می کنند .

لایه انتقال :

ابتدایی ترین وظیف این لایه آگاهی از وضعیت بسته ها می باشد که بسیار مهم نیز هست .
و در مرحله بعد وظیفه این لایه انتقال اطلاعاتی می باشد که نیاز به امنیت ندارند و سرعت برای آنها مهم تر است

لایه کاربرد :

این لایه دارای امکانات زیادی برای هنر نمایی متخصصان می باشد.

در این لایه برنامه های کاربردی قرار دارند و در کل این لایه ی نرم افزارهای شبکه می باشد و همچنین لایه پروتکل های نرم افزاری نیز می باشد .

از مهم ترین نکات در خصوص این لایه قراردادن : انتقال فایل (FTP) و مدیریت پست (SMTP) و بقیه برنامه های کاربردی می باشد .

پروتکل اینترنت IP

حتما همه شما عزیزان واقف به این موضوع هستید که IP یکی از مهمترین قسمتهای TCP/IP و شاید بتوان گفت مهمترین قسمت آن زیرا تقریبا شما برای هر کاری نیاز به آن خواهید داشت لذا بسیار ضروری و حیاتی می باشد که شما اطلاعات خود را در زمینه این مهم افزون کنید .

IP یک آدرس عددی است که برای ارتباط با شبکه به هر ماشینی در شبکه اختصاص داده می شود (چون IP برای وسایلی از قبیل ROUTER و MODEM و LAN و ... استفاده می شود ما اصطلاحا به جای نام بردن یک آن ها همه را ماشین می نامیم)

« IP شما نسبت به نوع اتصال شما متغیر و یا ثابت می باشد. »

وظیفه IP چیست ؟

وظیفه پروتکل IP حمل و تردد بسته های حاوی اطلاعات و همچنین مسیر یابی آنها از مبدا تا مقصد است

اساس کار پروتکل IP چیست ؟

IP پس از دریافت اطلاعات از TCP شروع به قطعه قطعه کردن آن به قطعه های کوچک به اسم FRAGMENT می نماید، پس از این مرحله برای هر FRAGMENT یک بسته IP می سازد که حاوی اطلاعات مورد نیاز بسته برای حرکت در طول شبکه می باشد و بسته IP را به بسته TCP اضافه می کند

و شروع به ارسال بسته های تیکه تیکه شده (FRAGMENT) می نماید حال مسیر یابی بر اساس تنظیمات قسمت IP بسته ها را به مقصد خود هدایت می کنند و آن را داخل زیر شبکه ها هدایت می کنند

خصوصیات IP :

بسته IP حد اکثر ۶۴ کیلوبایت فضا را اشغال خواهد کرد و بیشتر از آن نمی تواند باشد ولی موضوع جالب اینجاست که در حالت عادی حجم بسته حدود ۱۶۰۰ بایت بیشتر نمی شود

« بعدها یک حمله d.o.s بر مبنای همین موضوع طراحی شد »

IP در تمامی سیستم های عامل با ساختار استاندارد که دارد به درستی کار می کنند و نیاز به هیچ نوع سخت افزار ندارد .

بررسی ساختار بسته ساخته شده توسط پروتکل IP

بسته IP ساخته شده از تعدادی فیلد مجزا می باشد که هر کدام اطلاعاتی را در خود دارند که در زمان مورد نیاز این اطلاعات از داخل بسته ها استخراج می شود و مورد استفاده قرار می گیرد این اطلاعات شامل مواردی مثل آدرس IP فرستنده ، آدرس IP گیرنده و می باشد

بررسی فیلدها :

فیلد version:

وظیفه مشخص کردن نوع پروتکل IP را بر عهده دارد (در حال حاضر از دو version ۴ و ۶ استفاده می شود)

اندازه فیلد :چهار بیت

فیلد: IHL

وظیفه این فیلد نگهداری اندازه قسمت بالایی بسته در خود می باشد که از آن برای تعیین مرز بین اطلاعات و محتویات بسته IP استفاده می شود .

اندازه فیلد : ۴ بیت

فیلد :TYPE OF SERVICE

در این فیلد نوع سرویس انتقال تعیین می شود : ((کم سرعت و مطمئن))و ((پر سرعت و نامطمئن))

اندازه فیلد : هشت بایت

فیلد : TOTAL LENGTH

در این فیلد اندازه کل بسته IP قرار دارد که شامل قسمت سر آید و ناحیه داده می باشد که همانطور که گفته شد می تواند ۶۵۵۳۵ بایت باشد .

اندازه فیلد : ۱۶ بیت

فیلد : FRAGMENT OFFSET

این فیلد خود به سه بخش تقسیم می شود :

- ۱- بیت (DF(DON'T FRAGMENT) : اگر این بیت ۱ باشد هیچ مسیر یابی حق شکستن این بسته را ندارد
- ۲- بیت (MF(MORE FRAGMENT) : اگر این بیت ۰ بود به این معنی می باشد که این قطعه آخرین قطعه ارسال شده می باشد
- ۳- FRAGMENT OFFSET

در این قسمت شماره قطعه های شکسته شده قرار دارد و چون اندازه این فیلد ۱۳ بیت می باشد اطلاعات می توانند تا ۸۱۹۲ قطعه شکسته شوند (اندازه هر قطعه به غیر از قطعه آخری باید ضربی از ۸ باشد)

فیلد :TIME TO LIVE

همانطور که می دانید در این فیلد زمان سرگردانی بسته مشخص می شود و این به معنی می باشد که این بسته می تواند از چند مسیر یاب عبور کند که حداکثر آن ۲۵۵ می باشد . این فیلد یک نعمت بزرگ می باشد

اندازه فیلد : ۸ بیت

فیلد :PROTOCOL

در این فیلد شماره پروتکلی که قرار است بسته به آن برسد مشخص می شود

فیلد :HEADER CHECKSUM

وظیفه کشف خطا را بر عهده دارد

فیلد : SOURCE ADDRESS

این فیلد فیلد بسیار مهمی می باشد چون در آن آدرس مبدا موجود می باشد برنامه های فیلترینگ و فایروالها بسیار از این فیلد استفاده می کنند .

فیلد :DESTINATION ADDRESS

در این فیلد هم آدرس IP مقصد موجود می باشد

فیلد : OPTION

این فیلد یک فیلد خالی می باشد که در آن هر توضیحاتی به صورت دلخواه می توان نوشت

فیلد PAYLOAD:

در این فیلد داده ها بین لایه های مختلف رد و بدل می شود البته این امر از لایه های بالا به سمت لایه های پایینتر صورت می گیرد

نکاتی جالب در مورد IP

آدرس های ویژه :

این آدرسها نمونه های از آدرس های IP خاص هستند که از قبل برای مقاصد خاصی در نظر گرفته شده اند و در تعریف شبکه نمی توان از آنها به عنوان IP برای ماشینها استفاده کرد .

0.0.0.0

از این آدرس در مواردی استفاده می شود که ماشین میزبان از IP خود بی اطلاع است . البته اگر از این آدرس به عنوان آدرس فرستنده استفاده شود هیچ جوابی برای فرستنده پس فرستاده نمی شود .

HostId.0

این آدرس برای زمانی است که از آدرس خود در زیر شبکه بی اطلاع باشیم

255.255.255.255

از این آدرس برای ارسال پیامهای به صورت عمومی و فراگیر در شبکه استفاده می شود البته با استفاده از این آدرس می توان در زیر شبکه خود پیام فراگیر ارسال کرد .

NetId.255

از این آدرس برای ارسال پیامهای فراگیر در دیگر شبکه ها از خارج از آنها استفاده می شود . البته این سرویس تقریباً در بیشتر اوقات از سوی مدیران شبکه غیر فعال می شود .

در ادامه مباحث tcp/ip به بررسی ساختار فیلدهای بسته tcp و udp و و چند پروتکل مشهور خواهیم پرداخت
بسته tcp نیز همانند ip تشکیل شده از تعدادی فیلد می باشد که توضیحاتی در مورد شماره پورت مقصد شماره پورت مبدا و را در خود دارد حال به بررسی این فیلدهای مهم می پردازیم .

فیلدهادر بسته های tcp

فیلد source port :

این فیلد که مقداری برابر ۱۶ بیت دارد آدرس پورت(پروتکل) مبدا را در خود دارد با استفاده از این فیلد تقریباً می توان نوع داده های ارسالی را فهمید

فیلد destination :

در این فیلد آدرس پورتی که اطلاعات در مقصد باید تحویل آن داده شود موجود می باشد
این فیلد تعیین می کند که ما اطلاعات را برای چه پورتی ارسال می کنیم که البته در بیشتر موارد اطلاعات برای پروتکل های استاندارد ارسال می شود برای مثال پورت ۸۰ به صورت استاندارد پروتکل http را در خود دارد .

فیلد sequence number

این فیلد دارای عددی است که نشان دهنده تعداد بایتهای ارسال شده از داده ها است که این عدد با احتساب داده های بسته جاری در فیلد قرار می گیرد برای مثال اگر داخل فیلد عدد ۲۲۲۲۲۲ قرار بگیرد یعنی پس از ارسال بسته جاری ۲۲۲۲۲۲ بایت از داده ها ارسال شده است

فیلد acknowledgment number :

همانطور که از اسم این فیلد پیداست فیلدی است برای تصدیق کردن مقدار اطلاعات دریافت شده از طرف گیرنده برای مثال اگر در این فیلد که ظرفیت آن ۳۲ بیت می باشد عدد ۱۰۰۰۰۰۱ قرار داشته باشد به این معنی است که گیرنده دریافت اطلاعات تا این بیت را تأیید کرده و منتظر دریافت بقیه اطلاعات می باشد

فیلد tcp header length :

در این فیلد نیز عددی وجود دارد که مرز بین داده ها و سر آیند بسته را مشخص می کند
سر آیند به قسمتی گفته می شود که شامل فیلدهای TCP می باشد

فیلد Windows size :

در این فیلد مقدار فضایی که در طرف گیرنده خالی مانده است قرار دارد کاربرد این فیلد به این صورت است که مقداری که در این فیلد قرار دارد (مقدار فضای خالی بافر گیرنده) با مقدار داده ای که برای ارسال آماده است مقایسه می شود اگر بافر گیرنده فضای کافی داشته باشد داده ها ارسال می شود و در غیر اینصورت منتظر می ماند تا بافر گیرنده خالی شود و بعد اقدام به ارسال داده ها می کند

فیلد checksum :

این فیلد که فضایی ۱۶ بیتی را اشغال می کند حاوی کد خطاهای به وجود آمده در ارسال یا دریافت اطلاعات می باشد

فیلد Tcp segment length :

این فیلد مقدار کل بسته را بر حسب بایت در خود دارد

فیلد urgent pointer :

در این فیلد یک عدد که در اصل یک کد شبیه به کد وقفه ها است قرار دارد که در مواقع ضروری ارسال می شود

فیلد option :

این فیلد یک نعمت بزرگ می باشد در مواقعی که حجم بسته ضریبی از چهار نشود از این قسمت با داده های بی ارزش استفاده می شود تا مقدار ضریبی از چهار شود

بیت Urg :

این فیلد نشان دهنده وضعیت فیلد urgent pointer می باشد طرز عملکرد این فیلد ۱ بیتی به این شکل می باشد که اگر مقدار آن ۱ باشد به این معنی است که فیلد urgent pointer باید مورد ارزیابی قرار گیرد و اگر مقدار آن صفر باشد نسبت به آن فیلد بی تفاوت است

بیت ack :

اگر در این فیلد مقدار ۱ قرار گیرد دلیل بر اعتبار فیلد acknowledgment می باشد.

بیت PSH :

این بیت برای جداسازی بسته های حیاتی و مهم مورد استفاده قرار می گیرد این فیلد به گیرنده نشان می دهد که بسته حاوی آن باید سریعاً بافر شود و به برنامه کاربردی تحویل داده شود برای مثال در telnet

بیت RST :

این بیت برای قطع ارتباط مورد استفاده قرار می گیرد اما قطع ارتباط در این صورت یکطرف خواهد بود و ارسال داده ها ناتمام خواهد ماند و طرز کار آن به این صورت است که اگر حاوی ۱ باشد ارتباط را بدون اجازه و خبر دادن به طرف مقابل قطع می کند

بیت syn :

این بیت یکی از مهمترین قسمت های بسته tcp می باشد چون نقش برقراری ارتباط را بر عهده دارد

و اما آخرین بیت که بیت FIN می باشد :

این بیت تقریباً به معنای خداحافظی می باشد موقعی که یکی از طرفین داده ای برای ارسال نداشته باشد این بیت را ۱ می کند و این بدان معناست که این آخرین بسته ارسالی می باشد و بعد از ارسال بسته ارتباط به صورت یکطرفه قطع خواهد شد .