خب تو این بخش خیلی کوتاه اومدیم راجع به osi حرف بزنیم. او اِس آی مهم ترین و بزرگترین شرکت شبکه است. این شرکت که زیر مجموعه شرکت ایزو است وظیفه تعریف قوانین و استاندارد ها را در شبکه دارد. خب قبل از osi شرکت های فعال در حوزه آی تی وجود داشتن اما با این تفاوت که دستگاه هر شرکتی فقط با دستگاه های همون شرکت ارتباط میگرفتن و خب همونطور که مشخصه به خاطر روش ارسال و دریافت متفاوت دستگاه ها بوده. این شرکت اولین کاری که میکنه یک مجموعه قوانین طراحی میکنه و همه شرکت های فعال در این حوزه رو ملزم به اجرا اون میکنه.
این مجموعه قوانین که توی ۷ دسته متفاوت بودن یک روش ارسال و دریافت استاندارد ایجاد میکنه که باعث ایجاد ارتباط بین دستگاه های شرکت های مختلف میشه این قانون یک مدل ۷ لایه است که بهش میگن مدل osi. برای درک بهترش باید بگم این مجموعه قوانین تعیین میکنه هر بسته برای ارسال و دریافت ۷ تا کار باید روش انجام بشه. برای مثال لایه اولش که اسمش physical هستش مجموعه قوانین مربوط به کابل و سوکت و آنتن و فیبر و ... است. باز یه مثال دیگه میزنم برای درک بهتر موضوع مثلا ما توی لایه یک یه قانون داریم به اسم (.....) که تعیین میکنه کابل شبکه باید ۸ رشته یا ۴ زوج باشه یا سوکت شبکه باید ۸ تا پین داشته باشه و فلان مشخصات رو داشته باشه.
خب برگردیم سر مدل osi اول بیاید با هر لایه اشنا بشیم .

لایه ۱ physical :
همانطور که گفتم لایه یک مربوط به بخش فیزیکی یا مدیا یا همون رابط ها هستن که شامل کابل مسی، آنتن های رادیویی و فیبر نوری میشه. قوانین ظاهری، فیزیکی و حتی ساختاری.

لایه یک یه بحث فصلیه که اگر علاقه مندین پیشنهاد میکنم به بخش لایه یک کتاب comptia network+ مراجعه کنید اما چند تا مسئله مهم داره که من میخوام اینجا بگم.

اولیش کابل اترنت :
خیلی قدیم کابل شبکه کابل کواکسیال یا همون کابل آنتن تلویزیون یا دوربین های مداربسته آنالوگ بوده که هممون دیدیم. کابل کواکسیال یک رشته مسی که توی یه محافظ پلاستیکی ضخیم قرار گرفته (اون رشته های نازک دورش که توی بعضی از کابل ها هست فقط نقش نویز گیر رو دارن و برای انتقال اطلاعات استفاده نمیشن.) خب همونطور که مشخص بستر ارتباطی این کابل همون یه رسته مسی. این چه مشکلی ایجاد میکنه؟ بیاید با یک مثال به مسئله نگاه کنیم
فرض کنید اون سیم مسی یک لوله‌ست و بسته های شبکه یسری توپ دقیقا هم قطر لوله اند. خب اگر ما از دو طرف لوله توپ بفرستیم چه اتفاقی میوفته؟ تصادف میکنن پس کابل کواکسیال یک کابل یکطرفه است.
یعنی چی؟ یعنی نمیتونه امکان ارسال و دریافت همزمان رو ایجاد کنه.

همه ی اینارو گفتم که بگم مشکل کابل کواکسیال چی بوده که باعث اختراع کابل اترنت شده. ما نیاز به ارسال و دریافت همزمان داریم. برای اینکه ارسال و دریافت همزمان رو بهتر درک کنید به مثال های زیر توجه کنید.
بیسیم یک ارتباط یک طرفه است. یک طرف کلید رو نگه میداره و حرف میزنه و طرف مقابل فقط میتونه بشنوه و نمیتونه چیزی بگه. اما تلفن یک ارتباط دو طرفه است چون دو طرف میتونن همزمان صحبت کنن کابل اترنت به ما ارتباط دو طرفه میده. چطوری؟ کابل اترنت از ۸ رشته کابل نازک ساخته شده که ۸ تا رنگ مختلف دارن و هر کدوم یکاری میکنن. تا از این ۸ تا وظیفه ارسال بسته رو بر عهده دارن و ۲ تا از این ۸ تا وظیفه دریافت. کابل اترنت از طریق یک سوکت به دستگاه ها وصل میشه به اسم سوکت rj45
یچیزیه شبیه همون سوکت تلفن با این تفاوت که به جای ۴ تا پین ۸ تا پین داره

خب گفتیم کابل اترنت ۸ تا رشته رنگی داره پایین رنگ هاشو میگم بهتون
نارنجی - سفید نارنجی - سبز - سفید سبز - آبی - سفید آبی - قهوه ای - سفید قهوه ای
همونطور که احتمالا خودتون فهمیدید osi برای ترتیب این رشته سیم ها هم قانون داره.

ما دو تا قانون داریم که میگه این رشته سیم ها به چه ترتیبی توی سوکت rj45 چیده بشن. یکم جلوتر متوجه میشین که اگر با هر ترتیبی میخواین دو طرف رو به یک شکل سوکت بزنید سوکت کار میکنه اما این قوانین به دو دلیل رعایت میشن.
اول اینکه استانداردن و سوکت برای هر کسی که شبکه رو بشناسه قابل فهمه
دلیل دوم اینه که ما قبلا به دو روش کابل هارو سوکت میزدیم یکی straight یکی crossover و این دو روش از طریق استاندارد های بالا قابل اجرا بود. اسم این استاندارد ها a و b هستش.
رشته سیم ها تو سوکت rj45 شماره دارن. وقتی قفل سوکت رو به پایین باشه و ۸ تا پین رو به ما از چپ به راست سیم ۱ تا ۸ اند .
توی این ۸ رشته سیم های ۱ و ۲ وظیفه ارسال بسته رو برعهده دارن و ۳ و ۶ وظیفه دریافت.
۴ تا رشته باقی مونده برای انتقال برق استفاده میشن. بعضی دستگاه ها بخاطر محل قرار گیریشون امکان اتصال برق مستقیم بهشون نیست یا اگر هم هست، نگهداریش خیلی سخته؛ پس ترجیح میدیم با همون کابل شبکه برق دستگاه رو هم تامین کنیم که این کارو از طریق رشته سیم های ۴ ، ۵ برای فناوری poe یا power over ethernet و ۷ و ۸ برای فناوری poe+ استفاده میکنیم .
پی او ای اون فناوری ای هستش که به ما کمک میکنه از طریق کابل شبکه برق رسانی کنیم روش کارش اینطوریه که یک طرف کابل برق رسانی میکنه که میتونه سوئیچ یا روتری باشه که خودش این فناوری رو داره و پورت هاش علاوه بر شبکه، برق هم ارسال میکنن یا اینکه یک دستگاه وارد کننده poe یا poe injector میزاریم سر راه سیم و بهش آداپتور متصل میکنیم این کار باعث میشه سیم ما برق دار بشه

خب بالاتر گفتیم که به دو روش کابل اترنت رو سوکت میزیم یکی straight و یکی crossover تفاوت این دوتا تو اینه که کابل های straight دو سرشون با یک استاندارد سوکت میخوره مثلا دوطرف a یا دو طرف b اما کابل های کراس هر طرف یک استاندارد متفاوت داره یعنی یک طرف a و یک طرف b.
حالا این به چه درد میخوره؟ خب گفتیم که توی ۸ رشته، رشته های ۱ و ۲ وظیفه ارسال رو دارن و ۳ و ۶ وظیفه دریافت. پس اگر دو طرف با ۱ و ۲ ارسال کنن تصادف رخ میده. قبل ترها ما مجبور بودیم بین دستگاه ها کابل های کراس بزنیم که تصادف رخ نده اما امروزه دستگاه ها با هم مذاکره میکنن و مثلا میگن اگر طرف مقابل با ۱ و ۲ ارسال میکنه من با ۱ و ۲ دریافت میکنم و با ۳ و ۶ ارسال میکنم به خاطر همین امروزه دیگه کابل هارو straight استفاده میکنیم
تو بیشتر منابع توصیه شده که از کابل اترنت در نهایت مسافت ۱۰۰ متر استفاده بشه اما با این وجود امروزه کابل هایی داریم با فناوری cat 8 و cat 9 که میگن تا ۵۰۰ متر قابل استفاده است. من تصمیم گیری تو این زمینه رو به شما میسپارم میتونید راجع بهش سرچ کنید.

راجع به فیبر نوری و آنتن های رادیویی توی قسمت اول به اندازه نیاز توضیح دادم پس بریم سراغ لایه ۲
اسم لایه ۲ data link وظایف زیادی داره اما میشه گفت کارش وصل کردن لایه های بالایی که با منطق کامپیوتر و صفر و یک کار میکنن به لایه یک که بی منطق و با برق کار میکنه مثلا یکی از کارهاش نظارت به کار لایه یک برای اینکه ببین بسته ها سالم به مقصد رسونده یا نه. این لایه با آدرس مک کار میکنه که توی بخش اول کامل توضیح دادیم چطوری بسته ها با آدرس مک مسیریابی میشن و فهمیدیم که سوییچ دستگاهیه که لایه دویی کار میکنه. حالا میخوایم یکم بیشتر راجع به سوییچ و لایه ۲ حرف بزنیم .
خب اولین چیزی که خیلی مهمه بدونیم اینه که لایه ۲ یچیزی داره به نام هدر که به بسته ها اضافه میشه؛ توی این هدر آدرس مک مبدا، آدرس مک مقصد، تگ ویلن (همون تگ dot1q که قبلا راجع بهش حرف زدیم .) و .... .
اما چیزی که الان میخوایم توی هدر لایه ۲ راجع بهش حرف بزنیم اسمش fcs هستش که بعضی جاها crc هم بهش میگن .
حالا این fsc چیه؟ همون نظارت به عملکرد لایه ۱ . چجوری انجام میشه؟ خیلی سادست ولی برای فهمیدنش اول باید بفهمید که توابع در ریاضی چی اند؟ توابع یکسری ماشین عملگرا هستن که یک مقدار عددی واردشون میکنیم و تابع روی اون عدد یک عملیات مشخص انجام میده.
برای مثال تابع +۲ به هر عددی که بهش بدیم ۲ تا اضافه میکنه یا تابع ×۲ هر عددی که بهش بدین رو ضربدر ۲ میکنه.

برگردیم سر صحبت خودمون؛ بسته موقعی که ارسال میشه وقتی به لایه ۲ میرسه؛ لایه ۲ بعد از اینکه هدر بسته رو اضافه میکنه کل بسته رو میبره داخل یه تابع به نام crc و حاصل تابع رو به آخر بسته داخل خونهٔ fcs اضافه میکنه.
چجوری اینکارو میکنه؟ برای اینکه این موضوع رو بفهمیم اول باید اینو بدونیم که بسته ها توی هر لایه بجز لایه ۱ به شکل یه رشته بلند از ۰ و ۱ اند. پس ما میتونیم این رشته رو به عنوان یک عدد بزرگ ببینیم. لایه ۲ توی مبدا این عدد بزرگ و میبره تو تابع crc و حاصل رو میزاره توی fcs. دوباره توی مقصد وقتی بسته میرسه به لایه ۲ اولین کاری که لایه ۲ میکنه چک کردن fcs هستش؛ یعنی fcs رو جدا میکنه و خودش بسته رو میبره داخل تابع crc و اگر مقداری که به دست میاره با fcs مبدا یکسان باشه یعنی بسته تو مسیر تغییری نکرده ولی اگر متفاوت باشه یعنی اون رشته عدد بزرگ توی مسیر تغییر کردن پس بسته ما عوض شده پس اون بسته رو میندازه دور.

خب ما فهمیدیم که وقتی یک بسته به یک سوییچ میرسه اون سوییچ به جدول مک خودش مراجعه میکنه و برای عبور بسته تصمیم میگیره.
ببینید سوییچ ها عموما عملیات تصمیم گیری روی بسته انجام نمیدن و فقط بسته هارو رد میکنن. یعنی چی؟ یعنی سوییچ خودش تنظیماتی نداره که آقا مثلا این بسته از نظر من ممنوعه و دریافتش نکن پس سوئیچ فقط هدر لایه ۲ رو میخونه و بسته رو به پورتی که به مک مقصد متصل تحویل میده.

تو لایه ۲ ما یک مبحث مهم دیگه هم داریم به نام stp که مربوط به ارتباط بین سوئیچ هاست و از ایجاد loop در شبکه جلوگیری میکنه که این مبحث رو توی یک بخش جدا مفصل توضیح میدیم.
بحث دیگه ای که توی لایه ۲ داریم vlan که توی قسمت اول مفصل توضیح دادیم.

خب حالا وقتشه که برسیم به لایه ۳
لایه ۳ یا network مهم ترین وظیفش مسیریابی و مهمترین پروتکلش ip هستش
یچیزی که خیلی مهمه الان بفهمیم اینه که روتر بسته های برادکستی عبور نمیده پس میشه گفت انتهای دامنه برادکست هستش.
و چون بسته های برادکستی عبور نمیده میتونه توی دامنه های برادکستی متفاوتی باشه. یعنی چی؟ یعنی هر پورتش میتونه توی یه رنج متفاوت آی پی داشته باشه و بین رنج های متفاوت ارتباط کنترل شده برقرار کنه
خب حالا این به چه دردی میخوره؟ این مسئله به ما مفهومی میده به نام گیت وی.
فرض کنید من روی سیستم آدرس ۱۹۲.۱۶۸.۱.۱/۲۴ رو دارم و به یک سوییچ متصلم. بدون روتر با چه کسایی میتونم ارتباط بگیرم؟ فقط با هم رنج های خودم از طریق آرپ ارتباط لایه ۲ ای میگیرم؛ پس اگر بخوام با غیر همرنج خودم که مثلا اینترنت باشه ارتباط بگیرم باید چکار کنم؟ خیلی سادست باید بسته هامو بفرستم به اون روتری که به اون رنج یا مثلا اینترنت متصله. پس منم باید مستقیم یا غیرمستقیم مثلا از طریق سوییچ به اون روتر وصل باشم. اون پورت روتر که من بهش متصل هستم میشه default gateway یا دروازه من به شبکه های دیگه. برای همین میتونه شبکه های مختلف مثلا ۲ تا شهر رو به هم متصل کنه.

راجع به آدرسینگ و آدرس ها توی قسمت بعد خیلی مفصل و کامل حرف میزنیم

اما الان میخوایم خیلی کلی بگیم که آدرسینگ لایه ۲ یا همون مک فقط توانایی مسیریابی لوکال داخل یک لن رو داره یعنی چی؟ یعنی مسیریابی بین سیستم های متصل به یک سوئیچ یا چند سوئیچ متصل به هم.
اما مک آدرس نمیتونه دوتا شهر رو برای مثال به هم وصل کنه چرا؟ دلیلش خیلی سادست و تو قسمت بعد متوجه، میشید اما فعلا در همین حد تو ذهنتون داشته باشید که برای اتصال غیر لوکال ما به آدرسینگ لایه ۳ یا همون آی پی احتیاج داریم.
آی پی ها به ما اجازه میدن اون هارو گروهی مسیریابی کنیم که این برای ما حسن خیلی بزرگیه.

بالا گفتم مهمترین کار لایه ۳ مسیریابیه. یعنی چی؟
توی روتر که یک دستگاه لایه ۳ ای هستش ما یک جدول دیگه هم داریم (چرا یک جدول دیگه ؟ یعنی روتر ها جدول مک رو هم دارن چون به دستگاه لایه ۳ ای قطعا فهم و عملکرد لایه ۲ ای هم داره)
اسم این جدول، جدول مسیریابی که روتر ها برای عبور دادن بسته ها از خودشون به اون جدول مراجعه میکنن. البته در ۹۹.۹ درصد روتر ها ما یک جدول فایروال هم داریم که اگر بسته بتونه از اون عبور کنه به جدول مسیریابی میرسه. پیچیده شد؟ ساده ترش میکنیم.
توی روتر ما عملیات تصمیم گیری داریم. یعنی چی؟ یعنی ما میریم توی جدول فایروال روتر میگیم مثلا اگر آدرس فرستنده این بود بسته رو دریافت نکن یا دریافت کن علامت گذاری کن. حالا این شرطی که ما گفتیم آدرس مبدا (فرستنده) ۱۰۰ تا چیز میتونه باشه مثل آدرس مقصد ، پورت مقصد ، پورت مبدا ، پروتکل و...
خب این چکار میکنه؟ روتر وقتی بسته رو دریافت میکنه بعد از اینکه اطلاعات هدر لایه ۳ رو خوند بسته رو رد نمیکنه بلکه اول میره توی جدول فایروالش ببینه
این اطلاعات تنظیمات خاصی ندارن؟ عملیاتی که لازمه رو انجام میده و اگر اوکی بود تحویل جدول مسیریابی میده.
حالا کار مسیریابی شروع میشه. روتر مطابق با جدول مسیریابیش تصمیم میگیره که این بسته باید از کدوم پورت خارج بشه. خب این جدول چطوری پر میشه و کار میکنه؟ توی سوییچ ها اولین بسته ای که از یک پورت دریافت میشد آدرس مبدا خودش توی جدول مک ذخیره میشد و جدول مک کم کم به صورت خودکار تکمیل میشد مگر در مواقع خیلی خاص که ما مجبور بشیم دستی چیزی وارد کنیم که اونم فقط تو سوییچ های مدیریتی ممکنه. جدول مسیریابی روتر قصه دیگه ای داره
یکسری چیزها خودکار واردش میشه که اثر یکسری تنظیمات دیگه است.
یکسری چیز های خیلی زیادی رو هم دستی وارد میکنیم.

بالاتر گفتیم روتر میتونه توی رنج های مختلف آدرس داشته باشه.و ما میدونیم که اگر مثلا پورت ۱ روتر ما آدرس ۱۹۲.۱۶۸.۱.۱/۲۴ رو داشته باشه پس هر کس که توی رنج ۱۹۲.۱۶۸.۱.۰/۲۴ باشه به این پورت وصله. اینو از کجا میدونیم؟ از اون /۲۴ که بعدا مفصل حرف میزنیم .به این شبکه ها که خود ما یک آدرس توی اون رنج روی یکی از پورت هاش داریم شبکه های متصل میگن.
خب وقتی ما اینو میدونیم پس روتر هم میدونه. یکی از روش هایی که جدول مسیریابی خودکار تکمیل میشه همین روش یعنی ما به یک پورت آدرس میدیم و توی جدول مسیریابی شبکه اون آدرس ایجاد میشه.
روش دیگه تکمیل شدن خودکار جدول مسیریابی استفاده از پروتکل‌های مسیریابیه. پروتکل های مسیریاب به صورت خودکار شبکه های متصل به خودشون رو برای روتر های دیگه تبلیغ میکنن و یک شبکه پیوسته ایجاد میکنن.

روش دیگه ی تکمیل کردن جدول مسیریابی به روش دستی و ایجاد static route هستش. استاتیک روت ها ساختار های ساده ای دارن که دو قسمت کلی dst network و gateway را دارد.
قسمت اول میگه شبکه مقصدی که باهاش کار داری قسمت دوم میشه اون پورتی که از طریق اون به اون شبکه متصلی. توی مسیریابی چیزی که مهمه درکش کنید اینه که routing دو طرفه است و شما باید مسیر های رفت و برگشت ایجاد کنید و مسیر های یک طرفه کار نمیکنه.

بالاتر با default gateway آشنا شدیم ولی توی روترها ما این مفهوم رو نداریم و به جای اون از default route که یک static route است استفاده میکنیم.
در default route، شبکه مقصد ۰.۰.۰.۰/۰
و gateway آدرس روتر بالا دستی است که میتواند اینترنت باشد یا روتر مرکزی یا روتر لبه ای
پس اگر بخواهیم یک روتر اینترنت داشته باشد حتما باید در اون یک default route داشته باشیم تا ما رو به غیر هم رنج ها متصل کنه که مثلا اینترنت هم غیر هم رنج هستش.
توی لایه ۳ مفهوم بعدی که داریم qos یا مدیریت پهنای باند است که شاید بعدا مجزا بهش پرداختیم. اگر دوست دارید میتونید راجع بهش سرچ کنید. فعلا اینجا بحث لایه ۳ رو میبندیم و میریم سراغ لایه ۴

لایه ۴ یا همون transport

لایه ۴ وظیفه تعیین چگونگی انتقال داده ها رو بر عهده داره.
بزارید یک مثال بزنیم: فرض کنید که شما میخواهید یک بسته پستی رو از تهران بفرستید بندرعباس. این بسته تحت شرایط مختلف میتونه ارسال بشه. میتونه زمینی ارسال بشه، هوایی ارسال بشه، میشه موقع ارسال برای فرستنده پیام ارسال بشه یا موقع تحویل پیام ارسال بشه و ....
کار لایه ۴ دقیقا همینه. تعیین کنه این بسته به چه نحوی ارسال بشه. بسته ها پشت سر هم ارسال بشن و رسیدن یا نرسیدنشون مهم نباشه، یا هر بسته ای که ارسال میشه اول مقصد تاییدیه دریافت ارسال کنه و بعد ما بسته بعدی رو بفرستیم.
خب ما توی این لایه ۳ تا پروتکل مهم داریم که ۲ تاش خیلی معروفن و یکیش خیلی جدید
پروتکل های معروف UDP و TCP ان و اون جدید SCTP
خب حالا فرق اینا با هم چیه ؟ UDP میگه فقط بفرست مهم نیست که بسته ها میرسن به مقصد یا نه تو مثل یک اسلحه بسته هارو شلیک کن. اما TCP هر بسته ای که ارسال میکنه تاییدیه میگیره و مطمئن میشه که بسته به مقصد رسیده.
خب همونطور که احتمالا خودتون فهمیدین UDP قابل اعتماد نیست و TCP سنگینه پس یه پروتکل جدید ایجاد شده که مثل TCP قابل اعتماده و مثل UDP سبکه؛ اسمشم گذاشتن SCTP.
حالا بعضی جاها اصلا این تاییدیه گرفتن خوب نیست. چرا؟ چون TCP وقتی بسته ای ارسال نشه تو آخر ارتباط دوباره ارسال میکنه. بزارید یه مثال بزنیم.
فرض کنید دارید تلفنی صحبت میکنید و میگید : سلام چطوری ؟ خوبی؟
کانکشن شما از نوع TCP و سلام چ.... وبی ؟ ارسال میشه پس این وسط یکسری بسته از بین رفته که باید دوباره ارسال بشه.
پس طرف مقابل شما چی میشنوه؟
سلام چوبی؟ طوری
درسته؟ چون دقیقا بسته هایی که ارسال نشدن و دوباره اخرش میفرسته پس تو یسری از ارتباط ما ترجیح میدیم اگر بسته ای از دست رفت دیگه ارسال نشه که به ماهیت کلی بسته آسیب نرسونه. برای مثال توی ارتباط تلفنی یا برادکست تلویزیون بهتره که ارتباط UDP باشه تا به ماهیت ارتباط آسیب نزنه اما توی ارتباطی مثل دانلود فایل که بیت به بیت دیتا مهمه باید ارتباط TCP باشه.
توی لایه ۴ مباحث دیگه ای هم هست که برای سنگین نشدن مطلب بهشون نمیپردازیم شاید بعدا توی یک قسمت جداگانه بررسی کردیم.

میرسیم به لایه ۵ یا session
این لایه وظیفه برقراری جلسه بین مبدا و مقصد رو بر عهده داره و کلا به ۳ شکل ارتباط برقرار میکنه.
1. Simplex 2 .half duplex 3. Full duplex
سیمپلکس یعنی یکطرف همیشه فرستنده و یک طرف همیشه گیرنده
هف داپلکس یعنی در آن واحد هر طرف یا ارسال میکنه یا دریافت
فول داپلکس یعنی ارسال و دریافت همزمان.

لایه ۶ یا همون presentation کار آماده سازی بسته هارو انجام میده . اعمالی مثل رمزنگاری، هش کردن و .....

لایه ۷ یا application
وظیفه سرویس دهی و خدمت رسانی به یوزر رو بر عهده داره از طریق پروتکل های مختلف که توی یک قسمت جداگانه مفصل به این پروتکل ها میپردازیم