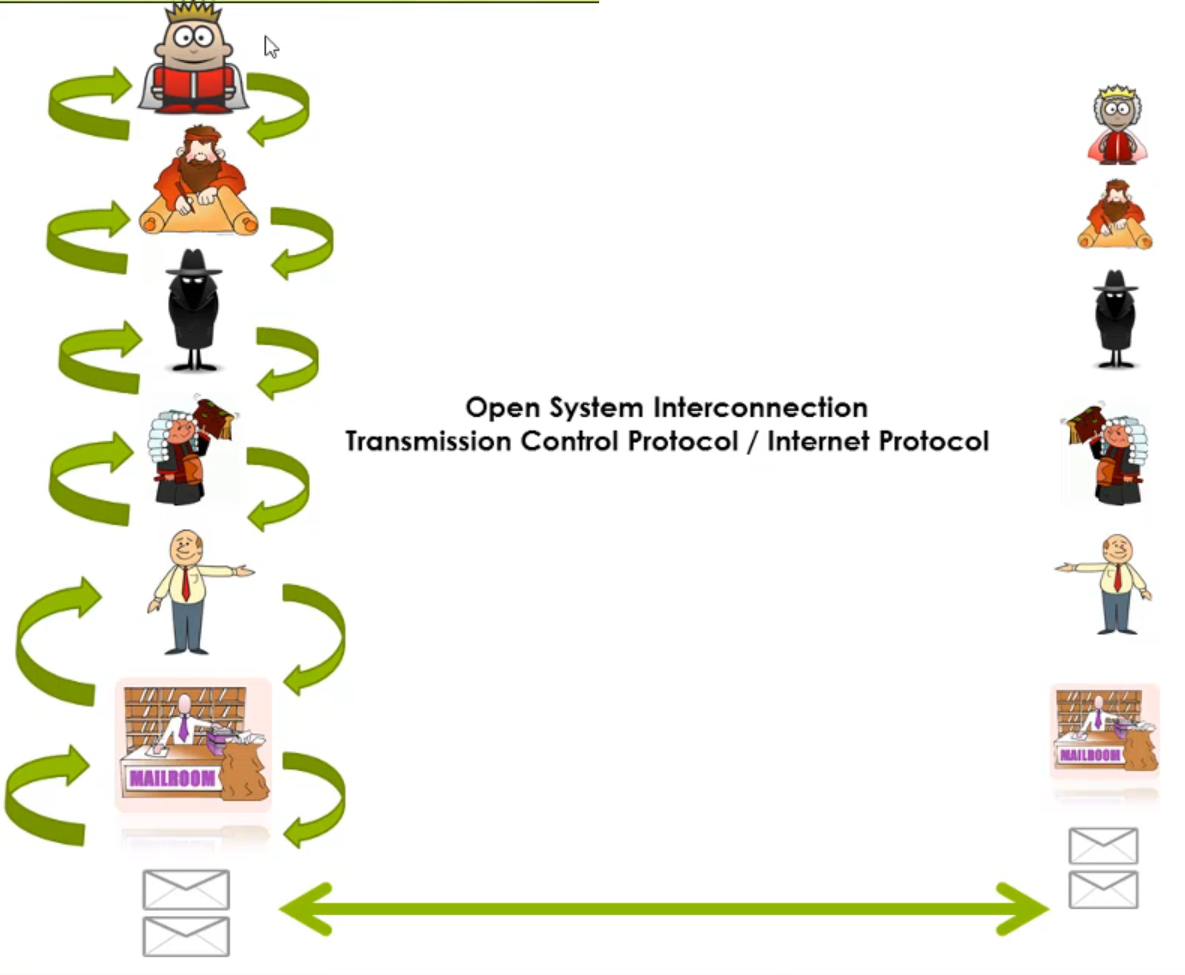
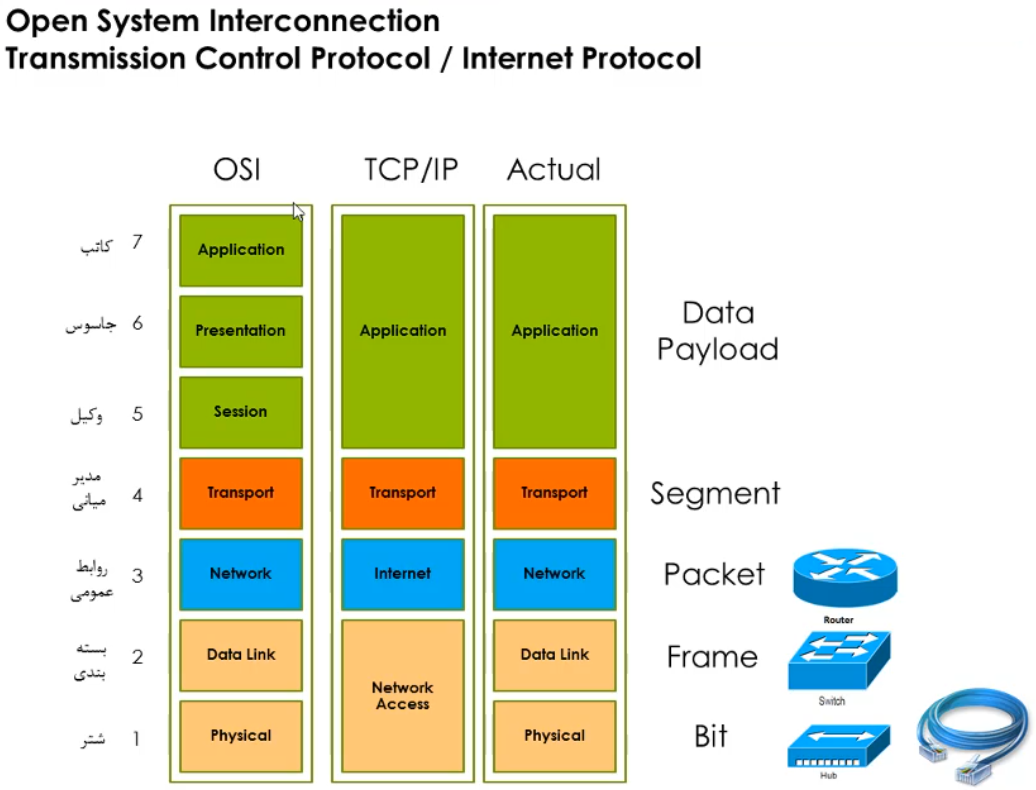
## تشریح لایه های osi و tcp/ip :



- هر کدام از اینها با نفر پایینی و بالایی خود یک ارتباط مستقیم و مستقل دارد و وظایف هر کدام در لایه ای که در آن قرار میگیرد مشخص شده است

- تفکیک شدن این لایه ها از این جهت ضروری است که مثلا اگر قرار باشد تغییری در یکی از قسمت ها ایجاد کنیم تنها باید آن لایه را تغییر و بهبود دهیم و لازم نیست تغییری در لایه های دیگر ایجاد کنیم نکته ی جالبش این است که لایه هایی که ارتباط مستقیمی که با لایه مورد نظر ما ندارند متوجه تغییر در آن لایه نمیشوند

- osi یک مدل مفهومی از شبکه میباشد به این معنی که شاید در عمل اتفاقاتی که در شبکه رخ میدهد دقیقا همان چیزی نباشد که در مدل osi وجود دارد . این مدل تنها برای درک بهتر انسان ها از شبکه طراحی شده است . این مدل یک مدل آکادمیک میباشد



- مدل osi درواقع تشریح میکند که اطلاعات در شبکه چگونه منتقل میشود

- پادشاه در مدل osi در واقع هر شخصی هست که قصد ارسال اطلاعات در شبکه را دارد که در بالای لایه ی application قرار میگیرد

- هر لایه برای خود پروتکل های مخصوص به خود را دارد که به روش های مختلف وظایفی که هر لایه بر عهده دارد را انجام میدهد

- هر گاه صحبت از سرویس یا خدمات میشود در واقع در مورد لایه ی ۷ صحبت میکنیم

- نام دیگر لایه ی ۷ user interface میباشد ( رابط کاربری )

- تنها لایه ای که کاربر میتواند با آن ارتباط برقرار کند لایه ی application میباشد

- در واقع کاری که لایه ۷ انجام میدهد ایجاد یک ارتباط با کاربر برای دریافت اطلاعات

- معروف ترین پروتکل های لایه ی 7 , http و dns و … میباشد

- وظیفه ی لایه ی presentation قالب بندی و فرمت دهی اطلاعات میباشد ( presentation = نمایش )

- قالب بندی در لایه ۶ به سه صورت انجام میشود یا رمزنگاری یا فشرده سازی یا تبدیل ( ترجمه ) میباشد

- به صورت فنی وظیفه لایه session ایجاد کردن , نگه داری کردن و پایان دادن به یک ارتباط میباشد

- در مدل osi وظیفه لایه ی transport این است که ببیند میزان اطلاعاتی که از لایه های بالاتر آماده است زیاد است یا کم اگر میزان این اطلاعات زیاد میباشد میبایست این اطلاعات را قطعه قطعه کنم .

- وظیفه ی دیگر لایه ی transport این است که باید مشخص کند که این قطعات در مقصد چگونه باید به هم متصل شوند به این وظیفه در واقع sequence number یا شماره گذاری گفته میشود

- وظیفه ی دیگر لایه transport نوع انتقال میباشد که برای ما سرعت مهم میباشد یا دقت . دقت به این معنی میباشد که در مقصد به ازای هر قطعه ای که دریافت کرد یک تاییده ی بگیر که این قطعه رسیده است به این حالت  
connection oriented گفته میشود . سرعت هم به معنی connection less میباشد . تفاوت در این دوحالت در این است که connection oriented به ازای هر قطعه یک تاییده میگیرد اما در connection less هنگام پایین session یک تاییده دریافت میکند (‌به ازای هر session ارتباطی تاییده میگیرند)

- یکی از کار های مهم لایه network مدل osi آدرس دهی میباشد که پارامتر آدرس دهی در این لایه ip میباشد به این صورت که آدرس ip مبدا و آدرس ip مقصد را قرار میدهیم به این نوع آدرس دهی logical address گفته میشود

- وظیفه مهم دیگر لایه network مسیر یابی یا routing میباشد

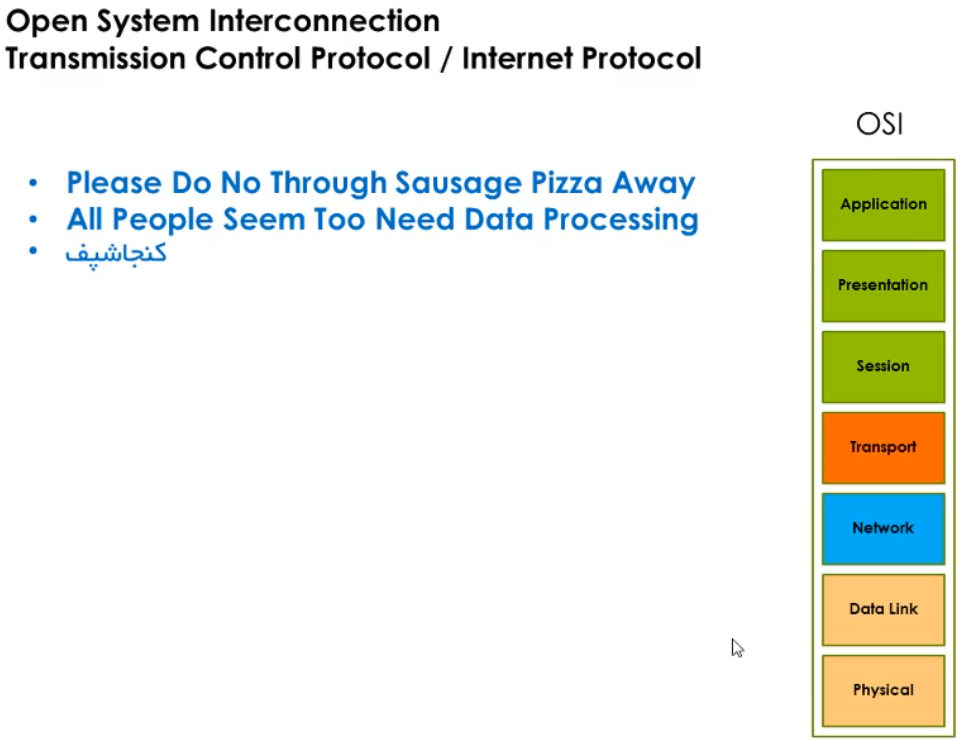
- در لایه ی data link دو کار انجام میشود یکی از این کارها درست کردن قالب اطلاعاتی میباشد کار دیگر این است که یک جور آدرس دهی دیگر هم در این لایه انجام میشود که به این نوع آدرس دهی physical address گفته میشود

- لایه physical وظیفه انتقال اطلاعات را بر عهده دارد ( تنها لایه ای که مستقیما با لایه ی متناظرش در اون سر شبکه ارتباط دارد لایه physical میباشد )

- مدل tcp/ip مدلی میباشد که در دنیای واقعی میتوان از آن استفاده کرد این مدل در واقع قابل لمس میباشد

- مدل actual دقیقا همان چیزی است که در دنیای واقعی رخ میدهد

- هنگامیکه اطلاعات از لایه های بالاتر به لایه های پایین تر انتقال پیدا میکند و آماده ارسال میشوند در واقع encapsulation صورت میگیرد و در طرف دیگر هنگامیکه اطلاعات از لایه های پایین تر با لایه های بالاتر انتقال پیدا میکند و آماده نمایش به کاربر میشود در واقع decapsulation صورت میگیرد

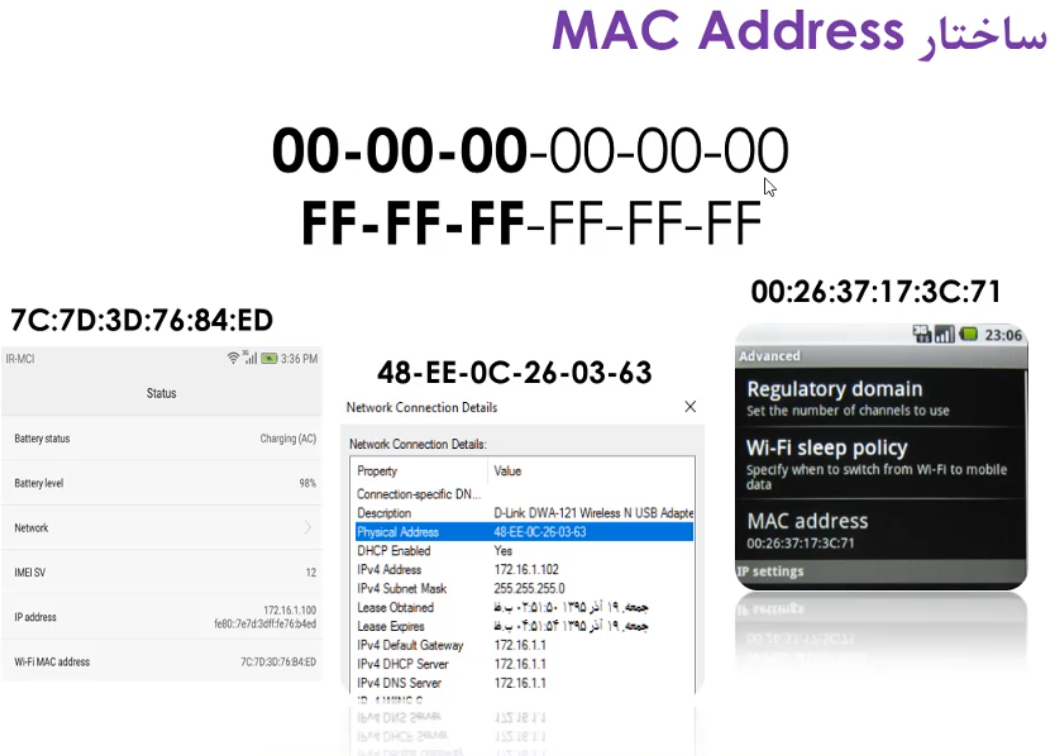


================================================================================

تفاوت آدرس دهی منطقی و فیزیکی :



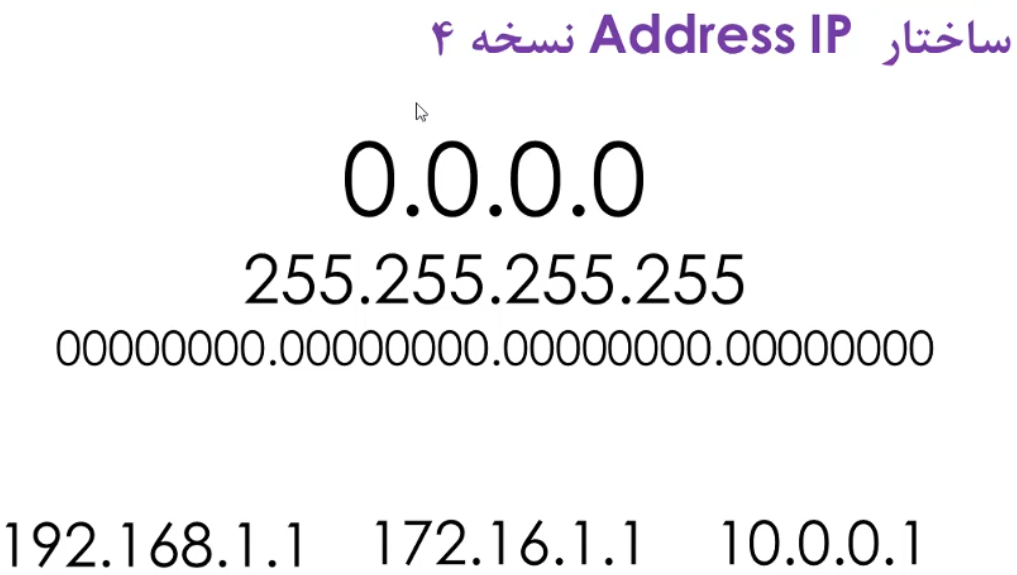
- به تعداد کارت شبکه هایی که به سیستم شما متصل شده است شما آدرس mac دارید اما به ازای هر آدرس مک شما میتوانید به هر تعداد آدرس ip داشته باشید

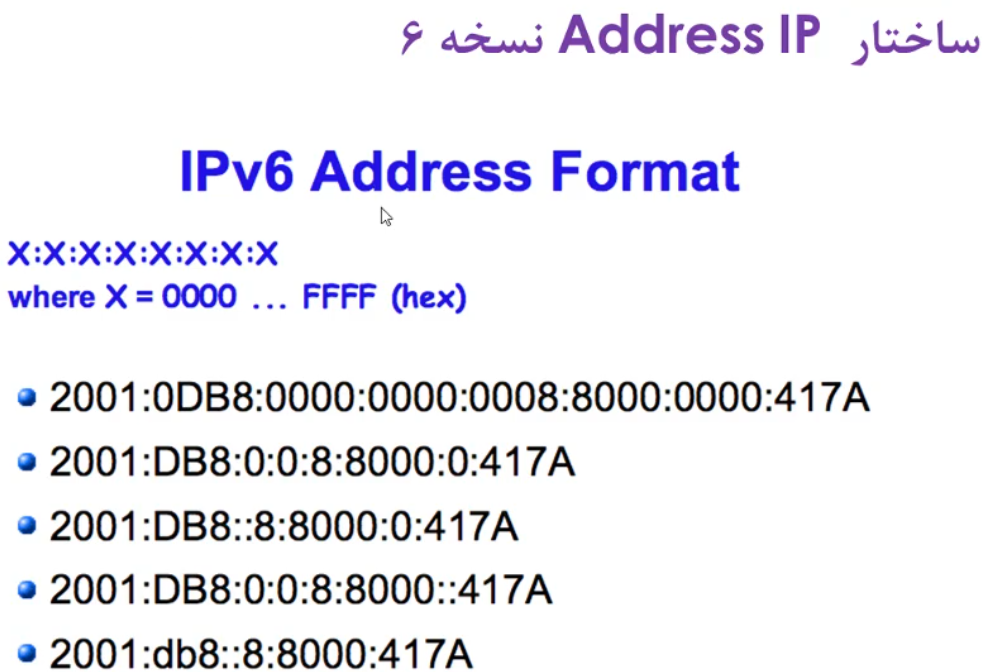


- ساختار آدرس مک به این صورت است که ۴۸ بیت میباشد و به ۶ قسمت تقسیم میشود و هر کدام از این قسمت ها در مبنای ۱۶ میباشد یعنی از صفر تا F

- ۳ قسمت اول آدرس مک در اصطلاح oui میباشد که شناسه ی منحصرد به فرد سازمانی میباشد به زبان دیگر ۳ قسمت اول به ما میگوید که این کارت شبکه ی شما ساخته ی کدام شرکت میباشد

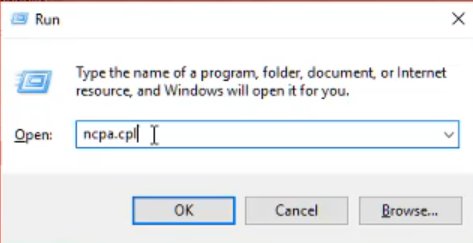
- ۳ قسمت دوم منحصرد به فرد میباشد و در دنیا نباید همانند آن وجود داشته باشد

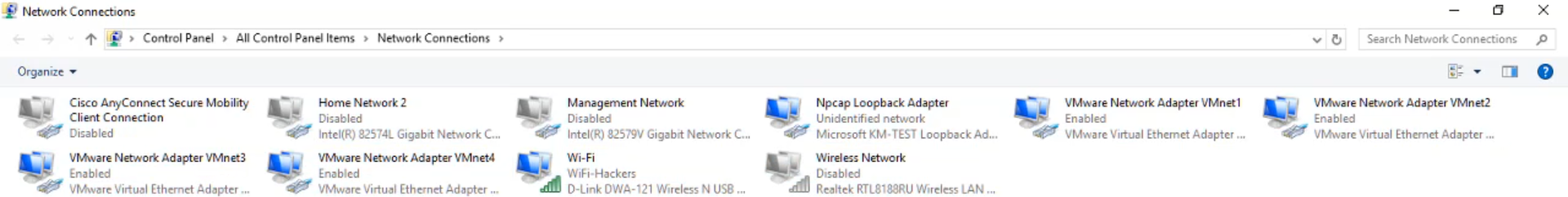
- ساختار آدرس ip به این صورت است که ۳۲ بیت میباشد و به ۴ قسمت تقسیم میشود که هر کدام از این قسمت ها در مبنای 10 میباشند و از صفر تا 255 میباشند ( به هر کدام از این قسمت ها اوکتت گفته میشود )



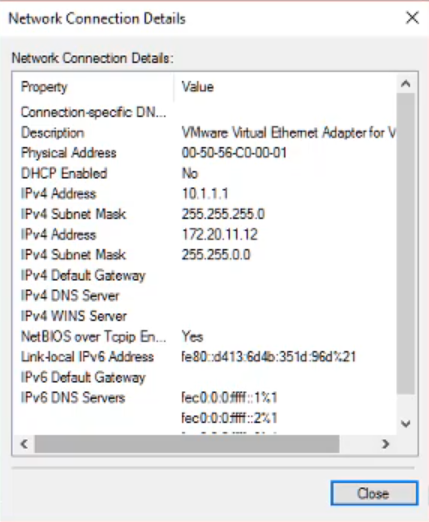
- برای اینکه بتوانیم در windows کارت شبکه های خود و آدرس های ip و مک هر کدام را مشاهده کنیم باید مراحل زیر طی کنیم :

۱. ابتدا کلید ترکیبی super+R را میفشاریم و عبارت ncpa.cpl را تایپ میکنیم ( ncpa = network connection panel )

  
2. بعد از فشردن کلید enter وارد همچین صفحه ای میشوید

آنهایی که آبی هستند فعال و آنهایی که خاکستری هستند غیر فعال میباشند

. نکته ای که بالاتر هم به آن اشاره شد این است که هر کارت شبکه تنها یک آدرس مک وجود دارد اما به ازای هر آدرس مک میتوانیم چندین آدرس ip داشته باشیم

  
- دستورات cmd که میتوانیم از آها استفاده کنیم :

. getmac = تمام آدرس های مکی که روی کارت های شبکه ی شما وجود دارد نمایش میدهد

ipconfig = آدرس های ip که در سیستم شما وجود دارد را نمایش میدهد

ipconfig /all = ‌تمام آدرس های سیستم شما (چه مک و چه ip) را نمایش میدهد

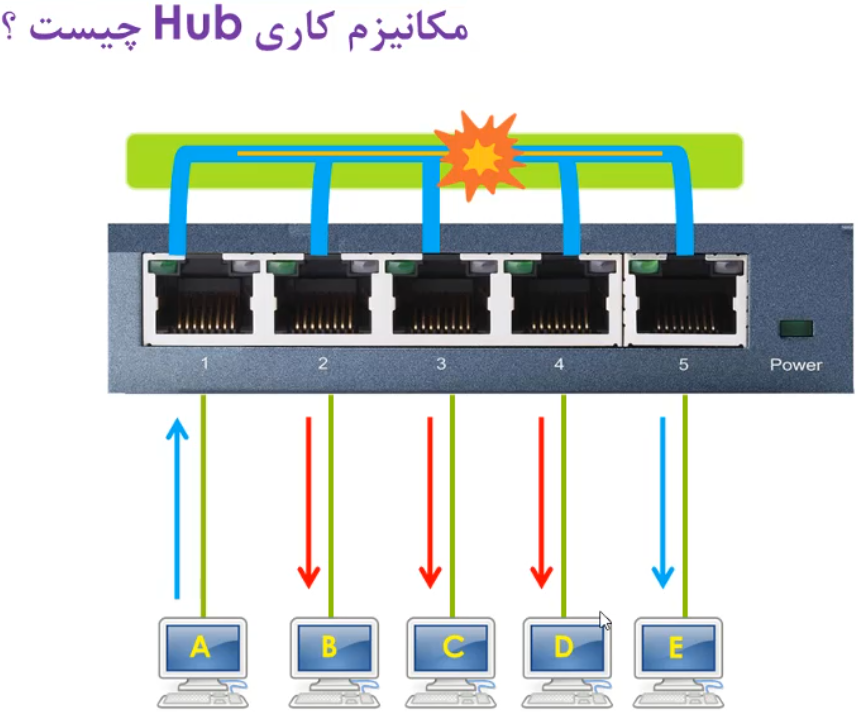
- از طریق آدرس های زیر میتوانیم متوجه شویم که آدرس های مکی که روی کارت شبکه ی سیتم ما وجود دارد از چه شرکتی میباشد

<https://macvendors.com/> <https://www.macvendorlookup.com/>

- با استفاده از نرم افزار mac address changer میتوانیم آدرس مک کارت های شبکه را تغییر دهیم

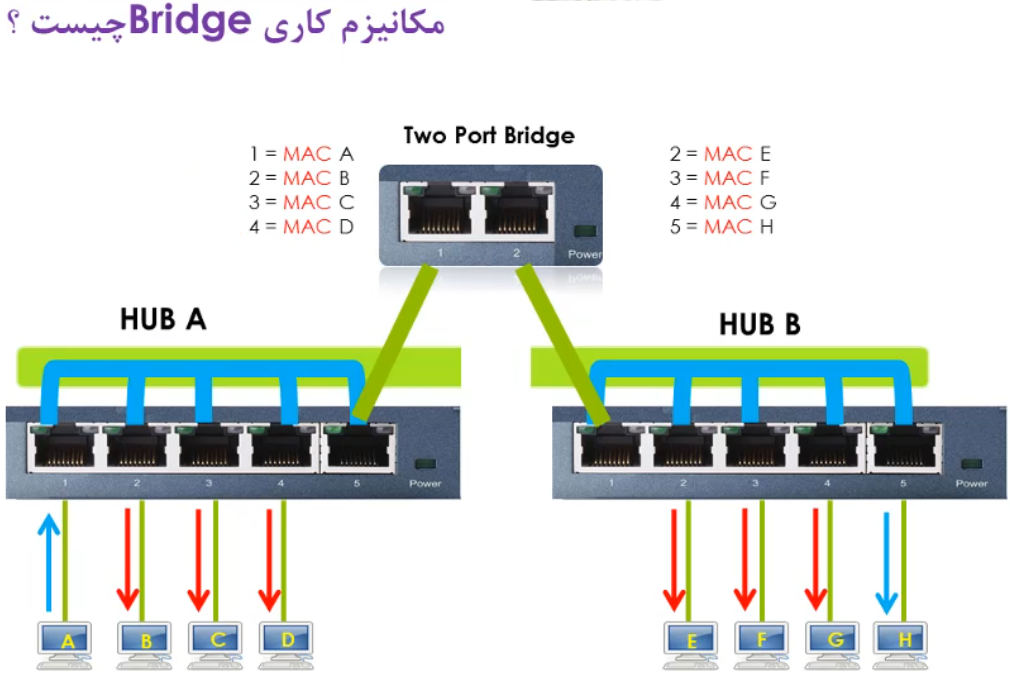
================================================================================

معرفی hub , switch و bridge :

  
- hub دستگاهی میباشد که در لایه ی physical مدل osi کار میکند به همین دلیل درک منطقی از آدرس دهی ندارد و به همین دلیل پهنای باند در hub به صورت اشتراکی استفاده میشود ( اگر کسی به ارسال اطلاعات مشغول میباشد دیگران باید صبر کنند که ارسال اطلاعات آن طرف تمام شود

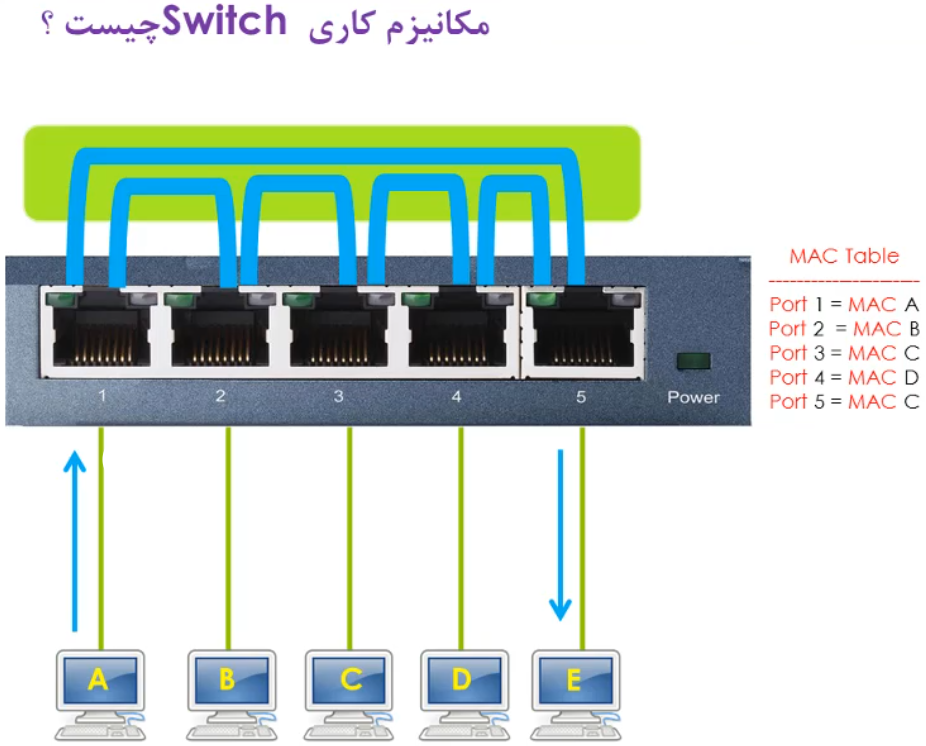
- از نظر امنیتی خیلی ضعیف میباشد

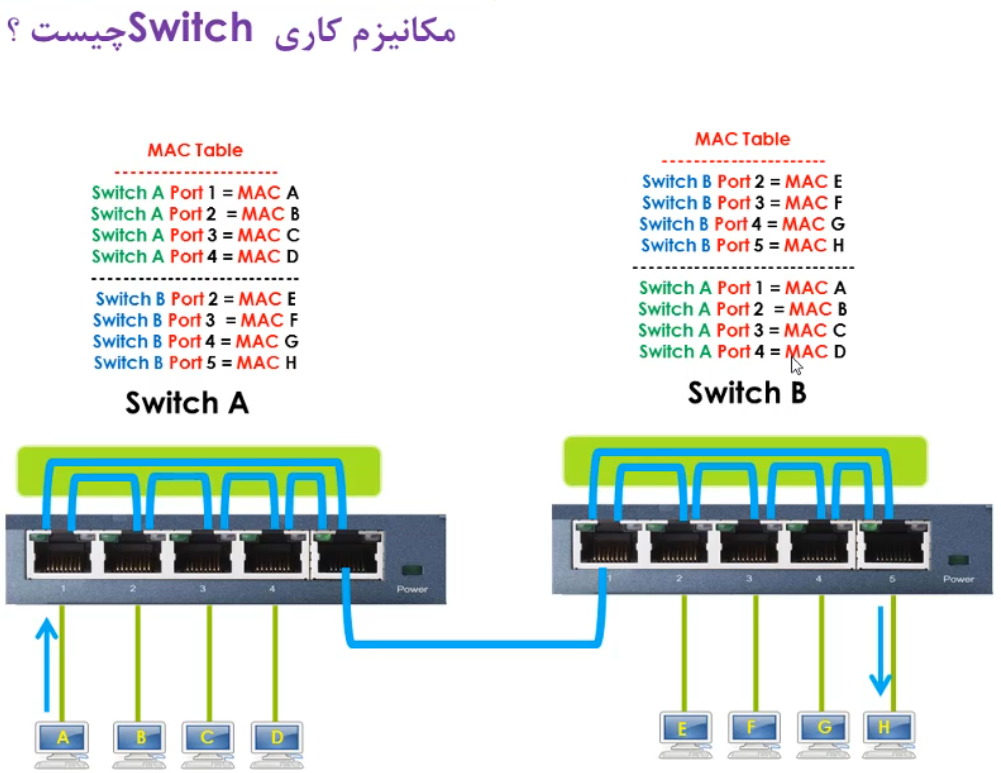
- اگر کامپیوتری به ارسال اطلاعات مشغول باشد و کامپیوتر دیگر شروع به ارسال اطلاعات کند تصادم یا collision رخ میدهد و hub از کار می افتد . تا زمانی که این مشکل برطرف شود به محدوده ای که با به وجود آمدن تصادم مختل شده است collision domain گفته میشود .



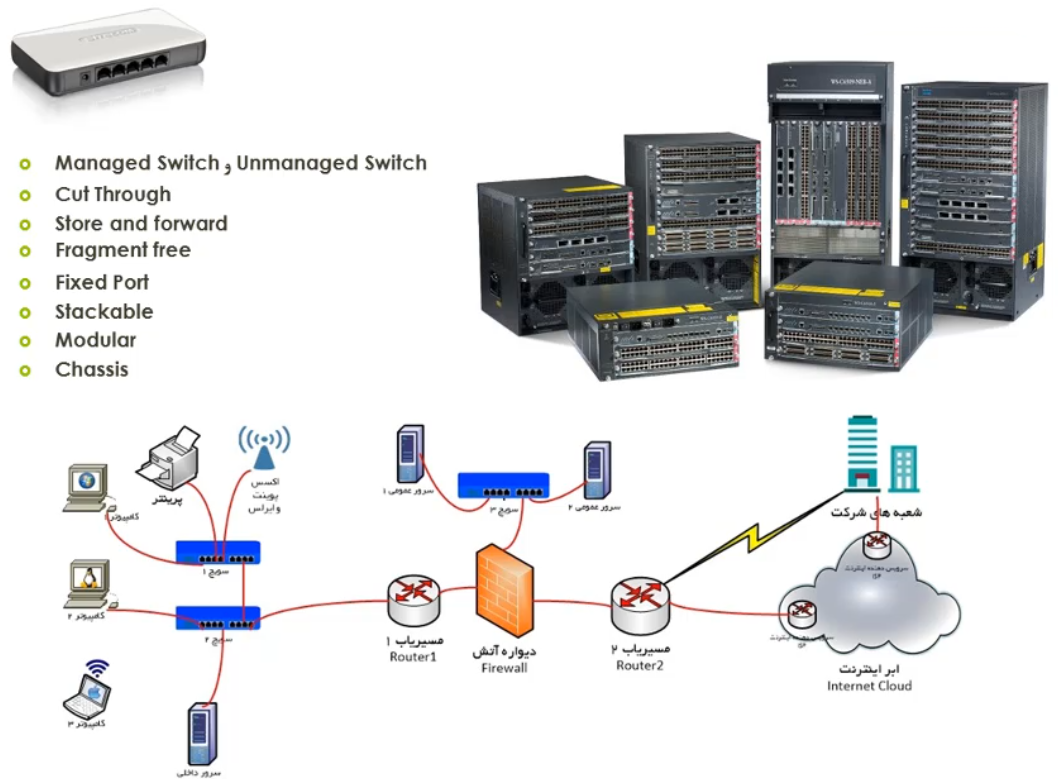
- اگر حالتی را در نظر بگیریم که پورت ۵ در hub a و پورت ۱ در hub b را با کابل به هم متصل کنیم هنگامیکه کامپیوتر A بخواهد اطلاعاتی را به کامپیوتر D ارسال کند این اطلاعات بصورت broadcast برای تمام کامپیوتر ها چه در hub a و چه در hub b ارسال میشود و این خیلی بد میباشد

- bridge بوسیله mac table ی که دارد میتواند این ارسال اطلاعات را کاهش دهد به این صورت که وقتی میبیند که بسته ی اطلاعات مقصد و مبداش در hub a میباشد دیگر اجازه نمیدهد این بسته ی اطلاعاتی در hub b برود ( نکته ای که از این مطلب میتوان برداشت کرد این است که دو collision domain وجود دارد به این صورت که اگر در hub a تصادمی اتفاق بیافتد bridge اجازه نمیدهد که این collision وارد hub b هم برود )

  
- switch یا multi port bridge به این صورت میباشد که از ویژگی خوب bridge که mac table میباشد استفاده میکند و آدرس mac هر کدام از کامپیوتر هایی که به switch متصل شده است را میداند به همین دلیل پهنای باند اختصاصی بین هر کدام از پورت ها وجود دارد به این معنی که اگر کامپیوتر a مشغول ارسال اطلاعات به e باشد کامپیوتر d هم میتواند به ارسال اطلاعات مشغول شود collision هم اگر در یکی از پهنای باندهای اتفاق بیافتد عملکر switch مختل نمیشود و باز هم بقیه ی پهنای باند ها آزاد هستند ( امنیت بالاتر میرود )



- مفهوم عکس بالا به این صورت میباشد که اگر بخواهیم دو switch را بوسیله cable به هم متصل کنیم , switch ها  
mac table های خود را به اشتراک میگذارند

  
- به طور کلی دو نوع switch وجود دارد managed و unmanaged که تفاوت های کلی آنها در آن است که سوییج های unmanaged غیر قابل پیکر بندی هستند و تنظیماتی که در آنها وجود دارد غیرقابل تغییر میباشد اما تنظیمات سوییچ های managed قابل تغییر هاست مثلا میتوان تنظیم کرد که پورت ۱ و ۴ نبایند باهم ارتباط داشته باشند یا حتی در این سوییچ ها میتوانیم الویت ترافیک تعریف کنیم ( در این سوییچ ها میتوانیم LAN های مجازی تعریف کنیم )

- دسته بندی دیگر cut through و store and forward میباشد به این صورت که در سوییچ های cut through با توجه به آدرس مقصد هر چیزی که وارد سوییچ شد بدون هیچ بررسی آن را از پورتی که مربوط به آدرس مقصد میباشد خارج میکند اما در سوییج های store and forward ابتدا در بافر های خود ذخیره میکند و بر اساس پهنای باند و سرعتی که کامپیوتر مقصد برای دریافت اطلاعات دارد این اطلاعات را از پورت خود خارج میکند

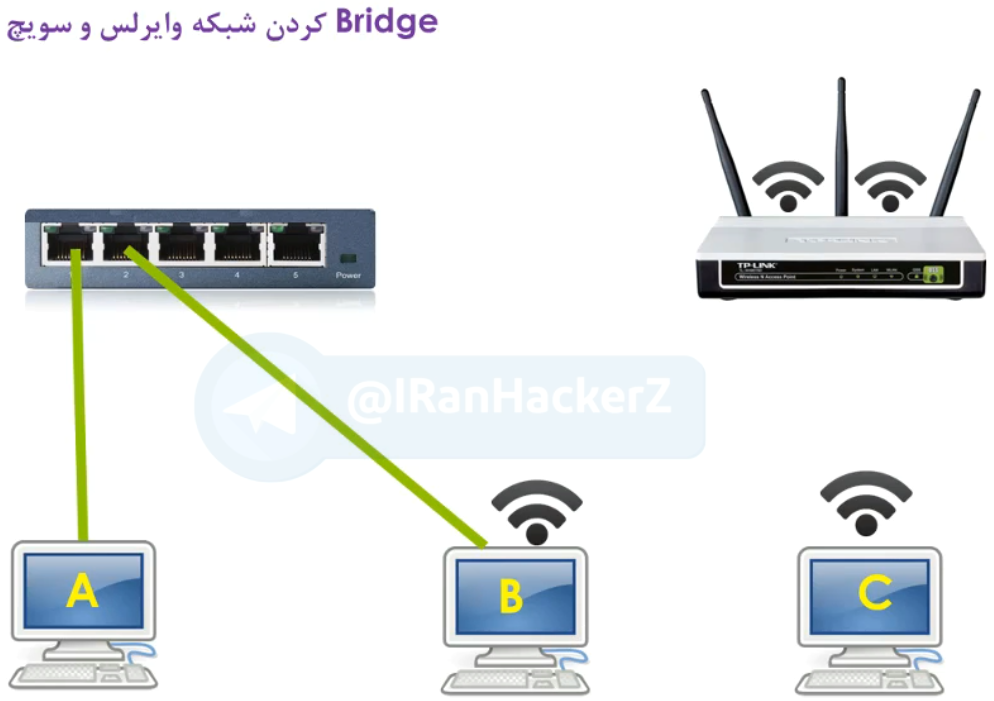
- fixed port نوعی از سوییچ میباشد که نمیتواند در تعداد پورت هایش تغییری ایجاد کرد

- stackable نوعی از سوییچ های managed میباشند که پورت خاصی را دارا میباشند به این صورت که میتوانیم از طریق این پورت ها دو سوییچ را به هم متصل کنیم و این دو سوییج به عنوان یک سوییچ کار کنند

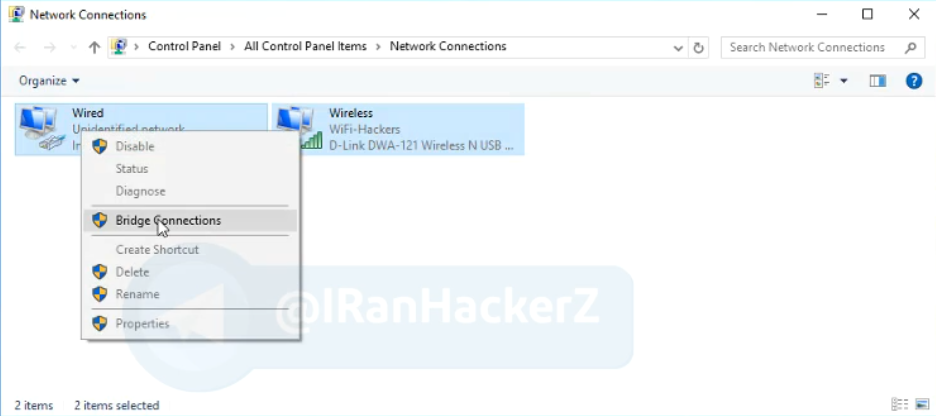
- modular نوعی از سوییچ ها میباشد که میتوانید امکاناتی را به این سوییج ها اضافه کنیم مثلا به عنوان فایروال عمل کند یا بتواند در لایه های بالاتر نیز فعالیت کند ( ip متوجه شود )

================================================================================

اتصال کردن شبکه کابلی به شبکه وایرلس با استفاده از bridge :



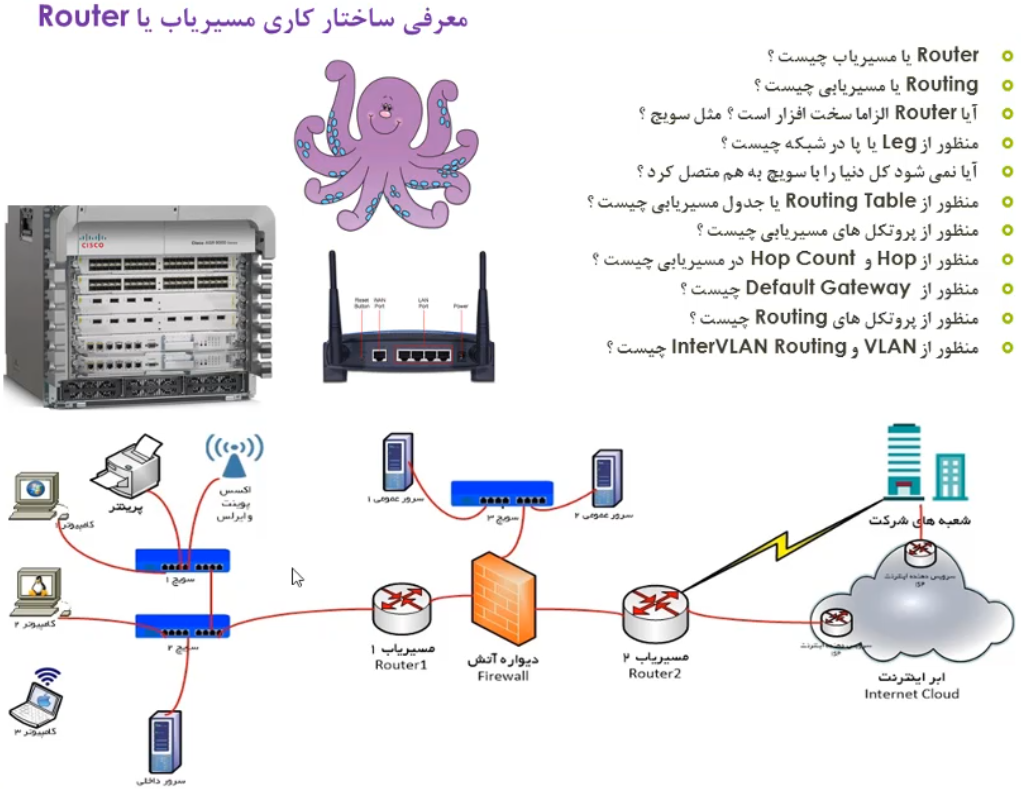
- در این مقال کامپیوتر B به عنوان واسط عمل میکند ( کامپیوتر B هم یک کارت شبکه بی سییم دارد و هم یک کارت شبکه کابلی )



- تصویر بالا نحوه ی bridge کردن در ویندوز را نمایش میدهد ( این کار باید در کامپیوتر B صورت بگیرد )

================================================================================

معرفی مسیریاب یا router :



- منظور از leg تعداد interfaceهای فعال router میباشد

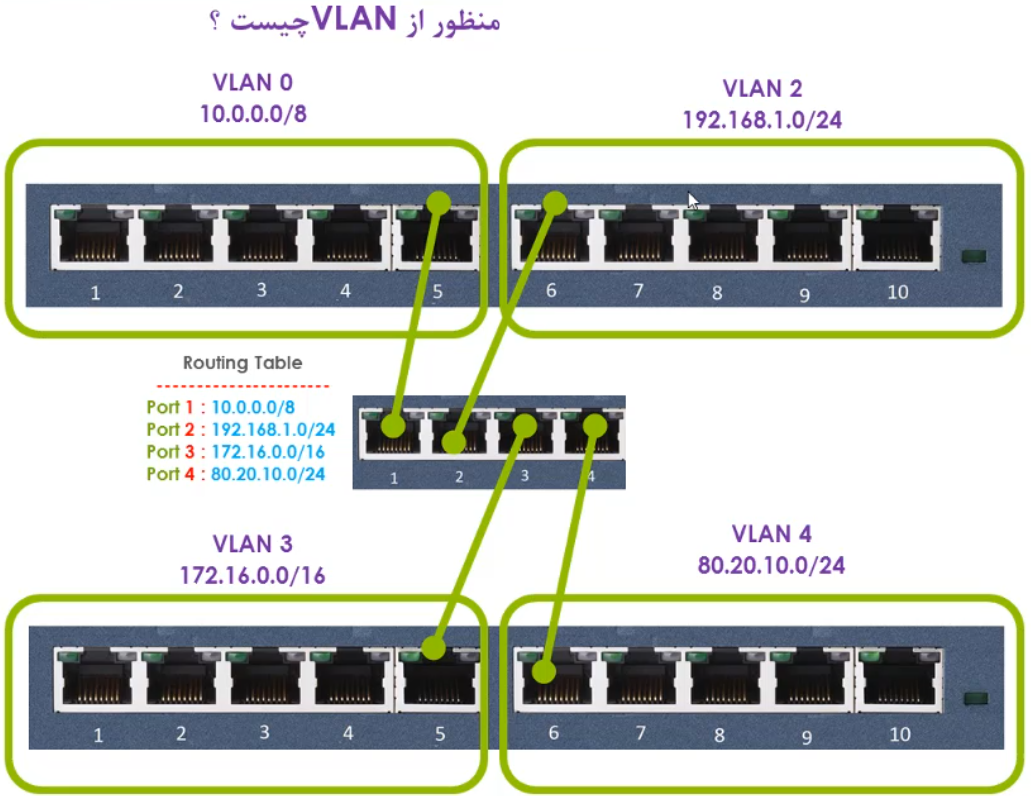
- switchها کامپیوتر ها را به هم متصل میکند اما routerها شبکه ها را به هم متصل میکنند

- منظور از hob یا hob count تعداد روترهایی که یک بسته ی ارتباطی طی میکند تا به مقصد برسد

- توضیح امروزی و بهبود یافته ی شبکه ی lan این است که تا زمانی که به یک روتر نرسیده ایم شبکه LAN گفته میشود

- مودم ADSL یک نوع از router میباشد

- پروتکل مسیریابی مهمترین و ساده ترین وظیفه شون بخش کردن routing table ها میباشد



================================================================================

دستورات ping و tracert :

- ICMP یک پروتکل احمق میباشد به دلیل اینکه اگر به مسیر مستقیمی یافت نکند دیگر تلاشی برای یافتن مسیر انجام نمیدهد

- همیشه اولین بسته ی ارتباطی ICMP مدت زمان بیشتری را طی میکند به دلیل این که در شبکه محلی برای اون آدرس IP جستجو میکند

- TTL یا time to live همان hip count میباشد به عبارت دیگر اگر تعداد hop count از تعداد TTL بیشتر شد router بعدی این بسته ی ارتباطی را دور می اندازد ( TTL ماکسیرمم hob countی هست که بسته ی ارتباطی میتواند طی کند )

- (t - ) سوییچ دستور ping میباشد که بصورت non stop به فرستادن بسته های icmp مشغول میشود   
 ( l - ) سوییچ دیگر دستور ping میباشد که میتوانید حجم بسته های ارتباطی را براساس بایت تغییر دهید  
 ( a - ) یکی دیگر از سوییچ های دستور ping میباشد که اگر بتواند اسم ipی سروری که ping شده است را برمیگرداند

- دستور دیگری که ماننده ping از پروتکل ICMP استفاده میکند tracert در ویندوز یا trace route در لینوکس میباشد کار این دستور مشخص کردن این است که بسته ی ارتباطی که میخواهد به مقصد برسد از چه سرور هایی عبور میکند ( عملکرد این دستور به این صورت است که هر بار ttl بسته ی ارتباطی را یکی زیاد میکند با این کار میتواند متوجه شود از چه router هایی عبور میکند )

ip2location.com open visual trace route monitis.com

================================================================================

تشریح مفاهیم firewall یا دیوار آتش :



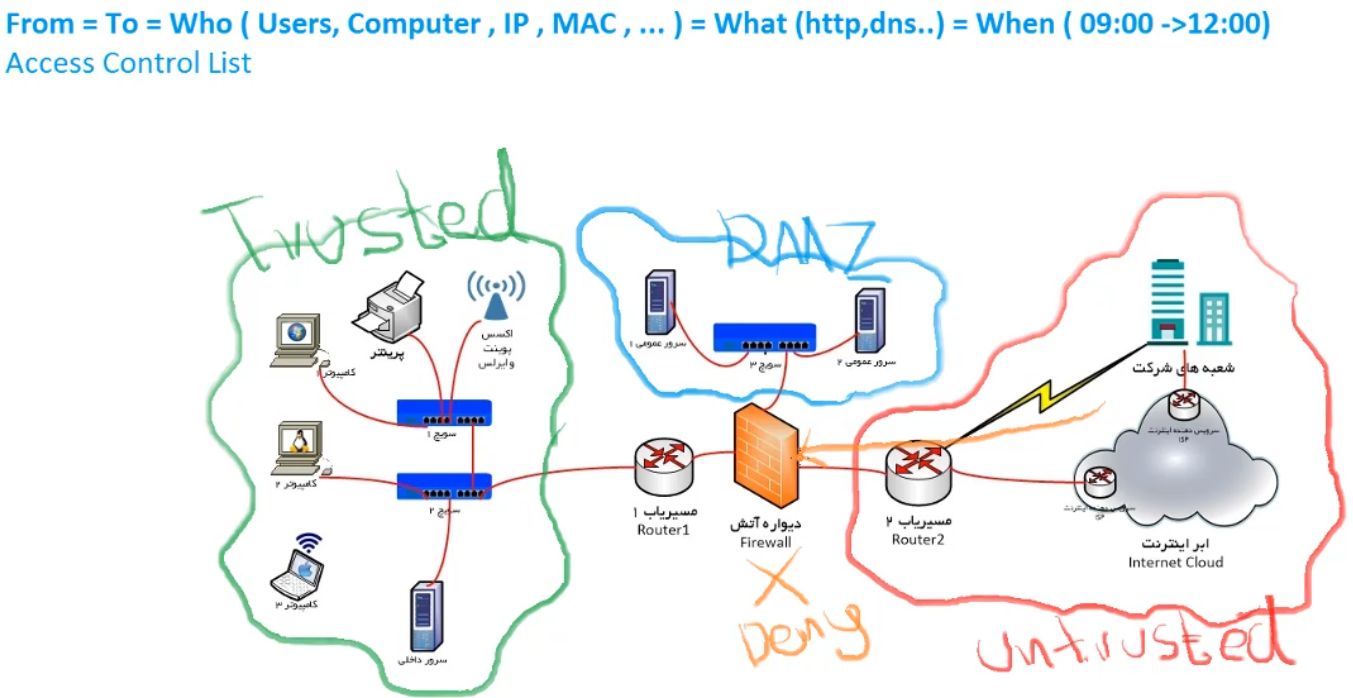
- firewall به زبان ساده نرم افزار یا سخت افزاری است که ما را از دسترسی های غیرمجاز خارجی محافظت میکند

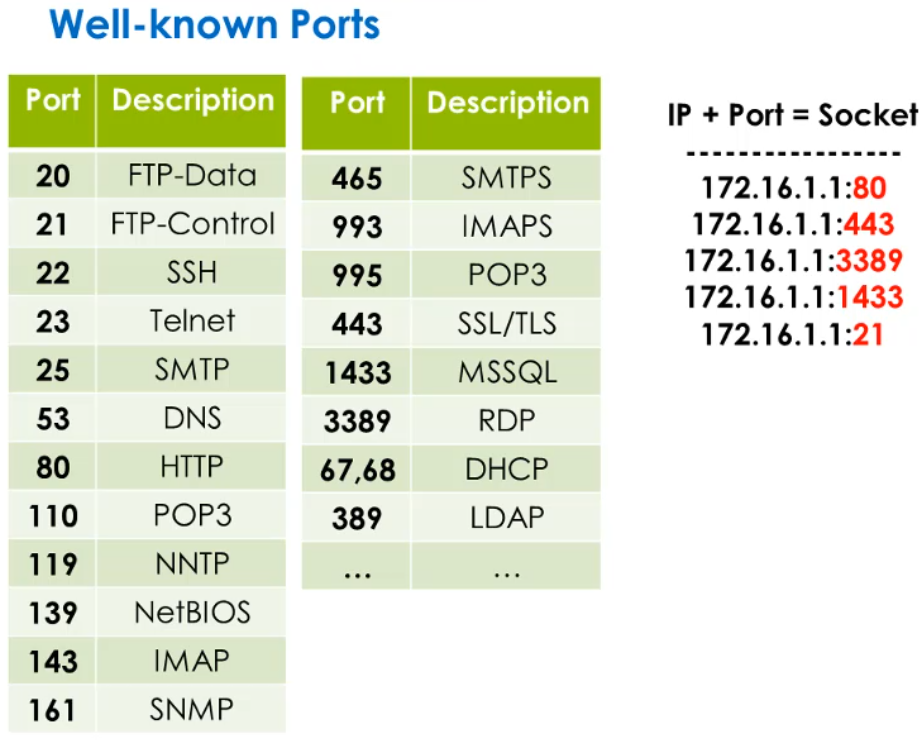
- به طور کلی فایروال یک نرم افزار میباشد یعنی اگر بتوانیم هزینه ی اضافی بابت سخت افزارهای فایروال نکنیم بهتر است چرا که آنها هم ماننده بقیه ی سیستم ها cpu و رم دارند و این نرم افزار برروی آنها نصب شده است

- zone یا area شبکه هایی هستند که به firewall ما متصل شده اند

- policy یا خط مشق یا سیاست و rule یا قانون در firewall به این معنی میباشد که چه چیزی اجازه ی عبور از firewall را دارد ( چه شرایطی اجازه ی عبور دارد ) مثلا اگر کسی از zone external روی پورت ۸۰ در داخل zone external درخواستی داشت اجازه ی ورود دارد اما برای دیگر پورت ها این امکان وجود ندارد

- اگر تمام دستگاه ها یا نرم افزار هایی که ما را دربرابر تهدیدات محافظت میکند را درون یک دستگاه قرار دهیم نام این دستگاه به صورت فنی UTM یا unified threats managements ( مدیریت یکپارچه ی تهدیدات ) نامیده میشود (‌به صورت کلی الان دستگاهی به نام فایروال در دنیا وجود ندارد اکنون تمام دستگاه ها utm هستند )

================================================================================



================================================================================